UNSOLVED!

The History and Mystery of the World's Greatest Ciphers from Ancient Egypt to Online Secret Societies

未解之谜

鲁道夫二世的私藏密码、
恺撒密码、黄道十二宫杀手密码……
揭示人类历史上那些未解的谜题

［美］克雷格·P. 鲍尔 著
（CRAIG P. BAUER）
鲁冬旭 译

（上）

中信出版集团

版权信息

书名:未解之谜（上）

作者:[美]克雷格·P.鲍尔

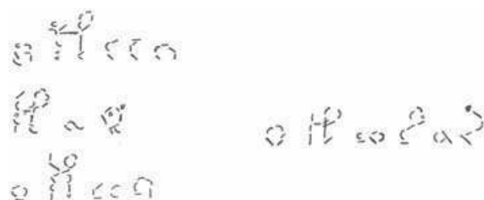
译者:鲁冬旭

ISBN:9787508695075

中信出版集团制作发行

献给勒内·斯坦和克劳斯·施梅，
我非常珍视他们给予的帮助和友谊。

前言



用密码写成的信息总是比每个人都能看懂的明显的文字信息更加有趣。虽然藏在密码伪装背后的也许只是一些非常无聊的信息，但是，在密码被解开之前，密码背后可能隐藏着任何东西：从价值数百万美元的宝藏的埋藏地点（第9章），到一位凶手甚至连环杀手的身份（第4、5、6章），再到可能改写历史的信息（第1、2章）。除此之外，还有另外一类有趣的密码，虽然这类密码背后不太可能藏有什么重要的信息，但是这些密码本身是几个世纪以来一直无人能解的谜团，因此无论是谁最终解开了这些密码，必会从此声名鹊起（第3、7、8章）。要解开这类密码，有时候必须依靠某种数学上的突破性发现，或者某种常人无法想出的创造性方法（第10、11章）。

在人类过去的解密历史中，有些密码是由在密码破译领域中有数十年经验的专家解开的［比如詹姆斯·吉洛格利（James Gillogly）和肯特·博克兰（Kent Boklan）］，也有些密码是被业余解密爱好者解开的［比如唐纳德·哈登（Donald Harden）和他的妻子贝蒂（Bettye）］。我相信，也许用不了多久，本书中的某些密码就会被我的读者解开。

在介绍历史上的各种未解密码时，也许按照时间先后顺序来介绍是最符合逻辑的做法。但是，要想了解为什么这些密码至今都未被解开，读者必须先了解破译密码的一般方法。为了向读者提供这些必要的密码

学背景知识，我在写作本书的时候没有按时间的先后顺序叙述。

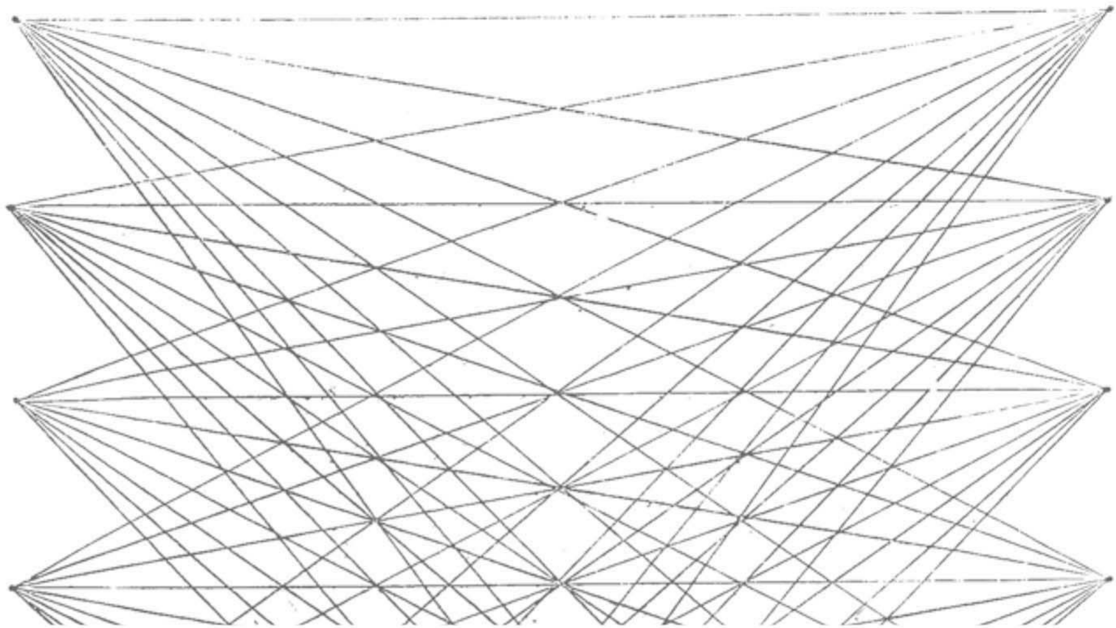
为了制造一些悬念，也为了防止读者产生“所有的密码都根本无法解开”的念头，我在本书中也会介绍一些已经被解开的密码。当然，我会先介绍密码的“谜面”，并讨论解法，最后才告诉读者谜底。这些已经解开的密码并不是我随便选出的一些例子——这些“已解之谜”事实上都能为我们所讨论的“未解之谜”提供一些启发。

当然，本书中介绍的这些尚未解开的密码也是在我的精心挑选之下才呈现在读者面前的。世界上现存的未解密码数目实在过于巨大，一本书的篇幅根本不可能把它们全部讲完。因此，在本书中我会尽量向读者介绍各种不同类型的密码，同时我也尽量避免提及那些涉及冗长技术讨论的密码。如果你最喜欢的密码没有出现在本书中，请不要生气，我随时欢迎读者向我提出建议，也许你喜欢的密码会出现在我未来的某一本书中。

书后列出的一些参考文献只有网络版本，这是不可避免的。如果在阅读本书的时候，我列出的链接已经无效了，你可以试试通过以下网址寻找相关的信息：https://archive.org/web/。有时候，虽然网页已经不存在了，但你也许还能通过上述网址找到网页的归档副本。

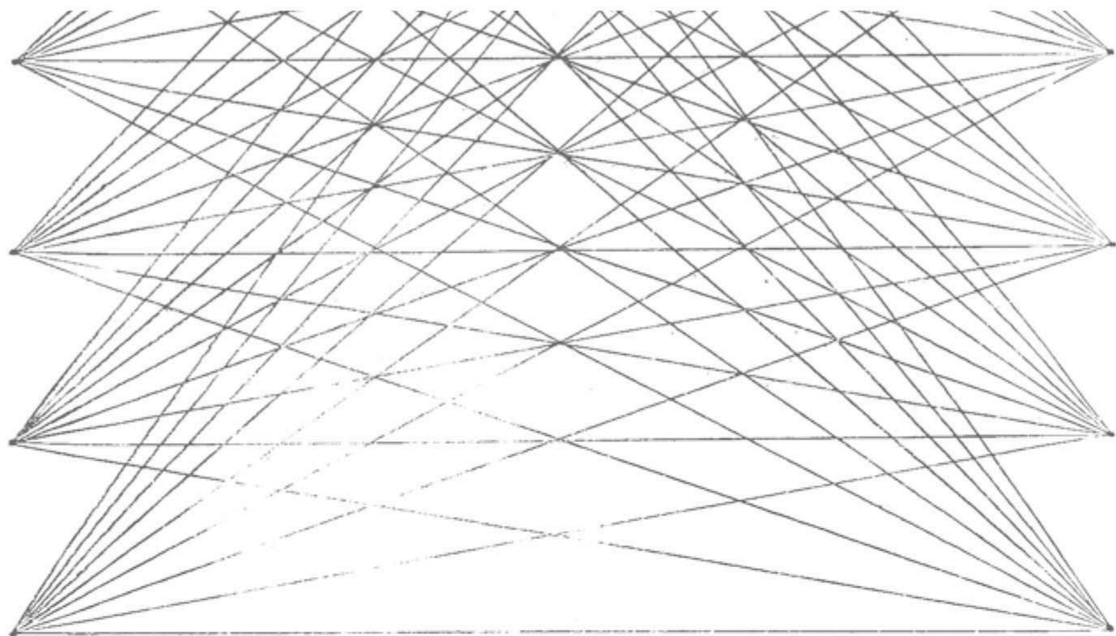
我的所有书籍都拥有良好的售后服务。如果你有任何问题想要询问我，可以向以下邮箱发送邮件：cryptoauthor@gmail.com。

表演就要开始了，祝你观赏愉快。

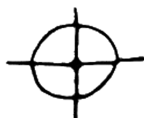


第 1 章

一位国王的探求



求知若渴



很多人都认为神圣罗马帝国皇帝鲁道夫二世（King Rudolf Ⅱ，1576—1612年在位）根本就是一个疯子。当时的天主教会甚至认为只有为他驱魔，才能解决这个棘手的问题。鲁道夫二世对治理国家并不上心，他将自己的所有精力都投入到炼金术之类的神秘事业中去了。鲁道夫二世的目标之一是找到传说中的魔法石（又称“哲人石”或“贤者之石”），据说拥有魔法石的人不仅能把其他金属变成金子，而且自己也能长生不老。为了达到上述目的，鲁道夫二世把他位于布拉格的城堡变成了一个炼金术与玄学的研究中心。鲁道夫二世不仅网罗了所有可以找到的玄学专家，而且只要是能帮助他达到上述目的的书籍和手稿，他都会不惜重金购买（甚至偷窃）。

在这些玄学书籍中，有一本书引起了鲁道夫二世的注意。这本书被称为《魔鬼圣经》。这本书的拉丁文名字是“*Codex Gigas*”，意为巨大的书——因为该书重达160磅（72.6千克），是世界上最巨大的手稿。到了13世纪后期，这本《魔鬼圣经》的内容已经混合了许多奇怪的内容：包括整部拉丁文《圣经》、希波克拉底的医学文献、布拉格的科斯马斯（Cosmas of Prague）所著的《波希米亚编年史》、一些魔法公式，以及一部关于驱魔的著作。传说这部奇书是一名获罪的僧侣靠魔鬼的帮助在一夜之间写成的。这位魔鬼的形象出现在这部《魔鬼圣经》的其中一页上，这一页的颜色比其他页都深，仿佛受到了某种来自地狱的能量的影响。

目前的主流观点认为，《魔鬼圣经》中包含魔鬼形象的那一页（以及其对开页）之所以会比其他页颜色深，只是因为该页使用次数远多于

其他页，因而接触了更多的阳光照射而已。对我来说，页面变深的这个所谓的“谜题”只用上述这句话就已经解开了。但是鲁道夫二世又购买了另外一本同样奇怪的手稿，而在这第二本手稿中又出现了一个更大的谜题。


AD SIT.
RVDOLPHVS II. DEI GRATIA ROM. IMPERATOR SEMPER. AVGVSTVS.

图1-1 鲁道夫二世

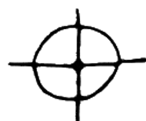
鲁道夫二世购买的第二本手稿尺寸较小，只有约6英寸[注]乘以9英寸见方。虽然鲁道夫二世可以轻松地随身携带这本手稿四处活动，他却根本没有办法着手研读这部手稿。首先，这部手稿没有封面。其次，这部手稿包含了200多页各种奇怪的符号，这些符号跟任何已知的字母表都不匹配，因此在这些奇怪的符号背后可能掩藏着任何东西。最后，这本手稿中还包含大量的图，我们有一定的理由假设这些图与手稿中的文字是相互关联的。但是，这些图像也可能是作者故意留在手稿中误导不知情的外行人的，作者的目的也许只是让这些外行人无法了解手稿的真正主题内容。

在讨论像这本书这样的古旧手稿时，收藏家们指代页码的时候通常不使用“页”，而是使用“叶”。手稿的每一“叶”包含前页（recto）和后页（verso）两个部分，因此收藏家们在标记页码的时候，首先注明该叶的序数，再用字母r或者字母v表示指代对象是前页还是后页。在鲁道夫二世的这本手稿中，有的叶的尺寸比其他叶大，因此这些大叶被多次折叠，以便保持和其他叶的大小相同。鲁道夫二世很可能是因为这本书稿中的插图才决定购买这本奇书的，因此，让我们首先来检视一下书中的插图。



图1-2 鲁道夫二世的巨书《魔鬼圣经》中的一页

一张图片胜过千言万语



这本手稿的开篇即是各种植物的素描图。在很多这类植物素描图中，图的周围填满了文字。这说明，作者首先绘制了这些插图，然后才添加了相关的文字。其中一个例子请见图1–3。当你观察图1–3的时候，请花一些时间仔细辨别，看看你是否能够辨认出图1–3中绘制的究竟是何种植物。很多人认为，这株植物的上半部分看起来像一棵向日葵。然而，向日葵的根系系统显然不是图1–3中所描绘的这个样子。事实上，图1–3中植物的根系部分看起来更像是马铃薯的根系。

事实上，除了向日葵和马铃薯以外，对这株植物的具体分类还有其他解读。圣玛丽山大学数学与计算机科学系的教授布赖恩·海因霍尔德（Brian Heinhold）就想到了另外一种植物，对此，他这样写道："在我看来，这株'奇怪'的植物看起来像一株菊芋。菊芋这种植物生长在世界上的某些地区，有时你也可以在菜店的农产品区找到菊芋的块茎。"注

不管图1–3中的这株植物究竟是什么，由于在手稿的这部分插图中出现了各种各样的植物素描图，所以研究者把手稿的这一部分称为"草本/植物学部分"。



图1-3 手稿的第33v叶（草本/植物学？）

在草本/植物学部分之后，这部手稿中又出现了另外一种类型的插图。这些插图被认为与天文学或占星术相关。图1–4就展现了这类插图中的一幅（该图在原书中因为太大被折叠了起来）。在图1–4中，左边的这个物体可能代表太阳，因为从这个物体中射出了12道光线。在每两道光线之间，我们可以看到一个实心的三角形，和另一个内部画有星星图案的三角形。每个三角形中所包含的星星图案的数量各不相同，这种数量上的差别可能具有某种重要的意义，但是我们并不清楚这种含义究竟是什么。然而，我们知道数字12是与太阳相关联的，数字12很可能代表着十二星座。

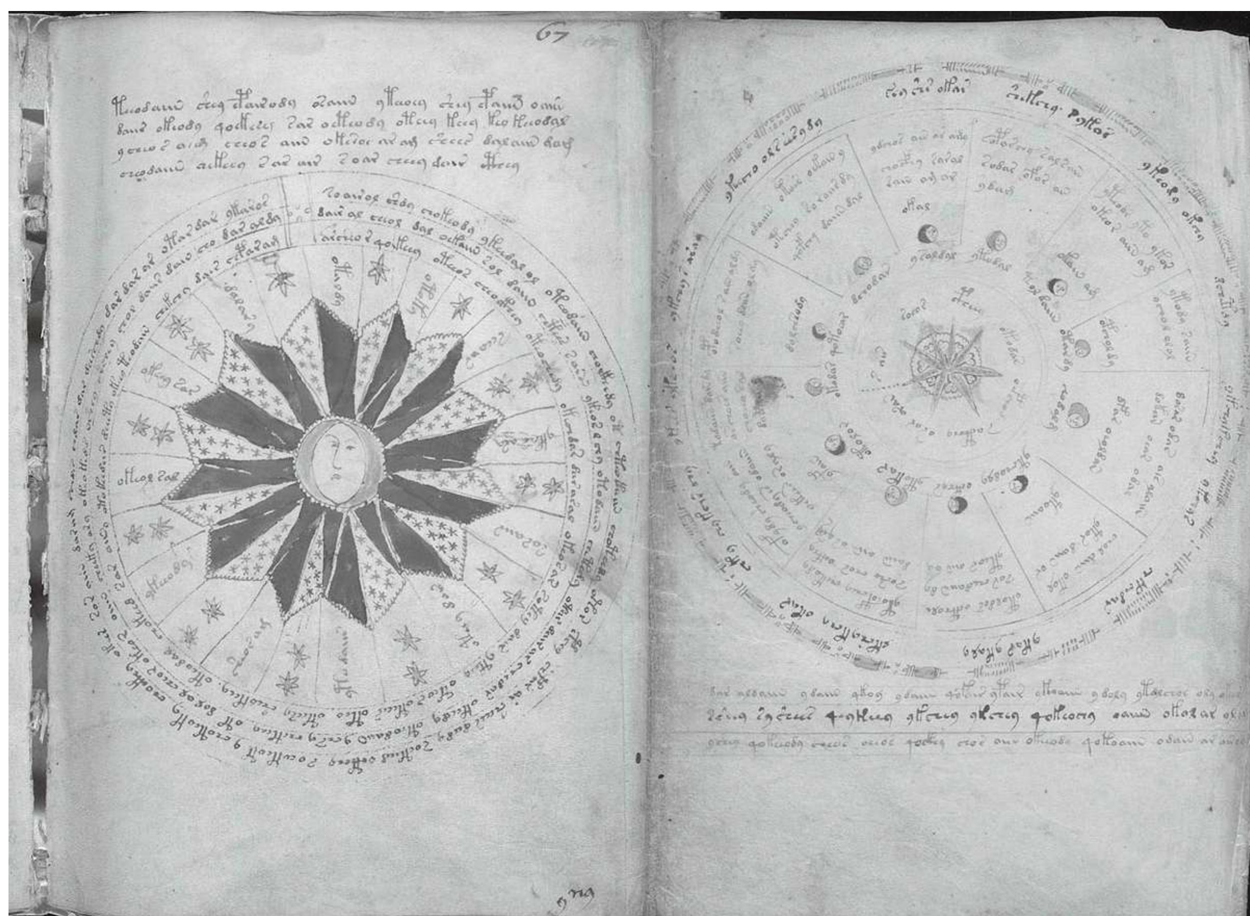


图1-4 手稿的第67r叶（天文学/占星术？）

在天文学/占星术部分之后，我们又进入了手稿的下一个部分。让我们暂时把这个部分叫作“生物学部分”。手稿的生物学部分包含了许多裸体女人的图，这些裸体女人站在一些桶一样的物体中。我们可以看到

图中的水或者其他某种液体在流动。这些插图描绘的是人类的循环系统吗？或者，有没有可能这些插图描绘的其实是某种管道排水系统呢？

在生物学部分结束以后，我们看到了这部手稿中可能最奇怪的一个部分。在图1–6中，左图的中心似乎是一个太阳，而右图的中心可能是一个太阳或者一轮新月。因此，我们有理由把这个部分叫作“宇宙学部分”。然而，如果我们相信这部分插图描绘的确实是与宇宙学相关的内容的话，我们又如何解释接下来的这个巨大的折页呢？研究者对接下来的这个巨大的折页提出了许多不同的解读方式。

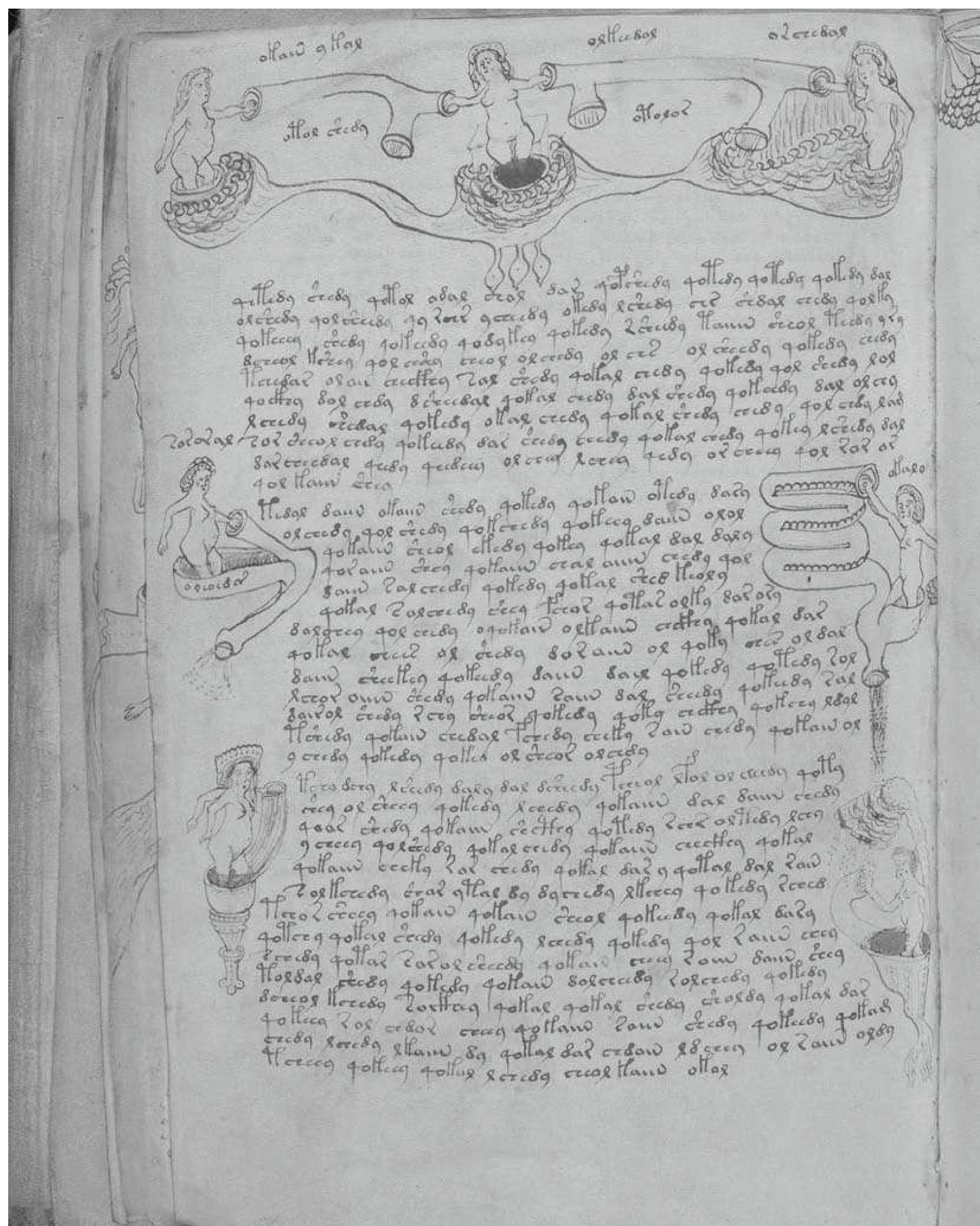


图1-5 手稿的第77v叶（生物学？）

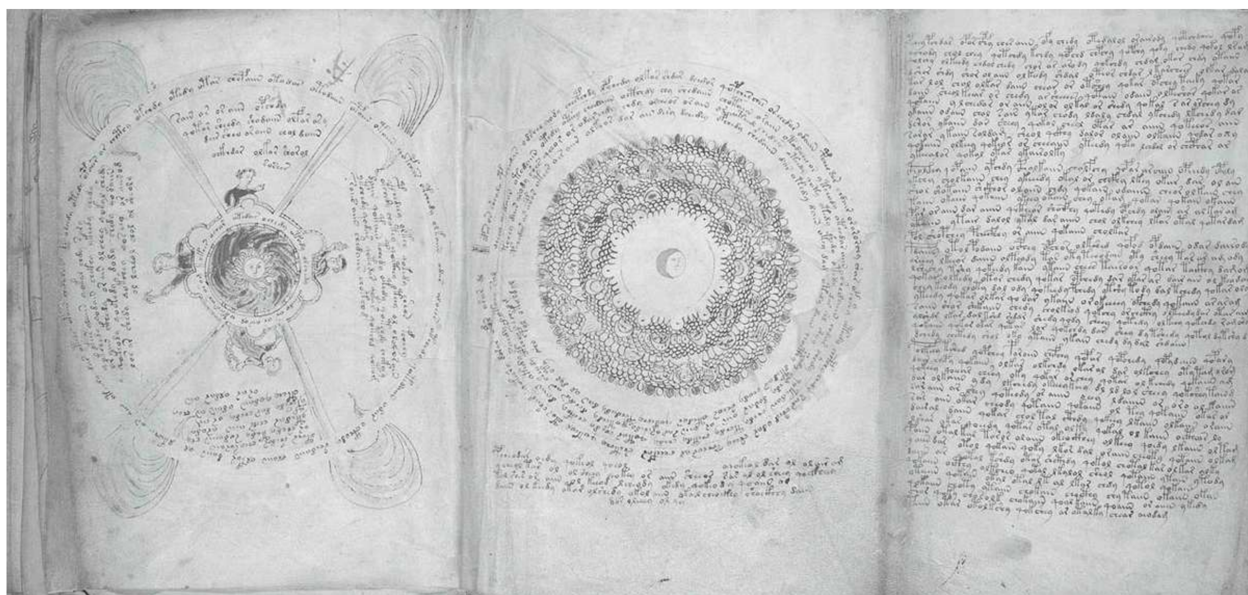


图1-6 手稿的第85r叶（局部）及第86v叶（局部）
（85~86折页的一部分）（宇宙学？）

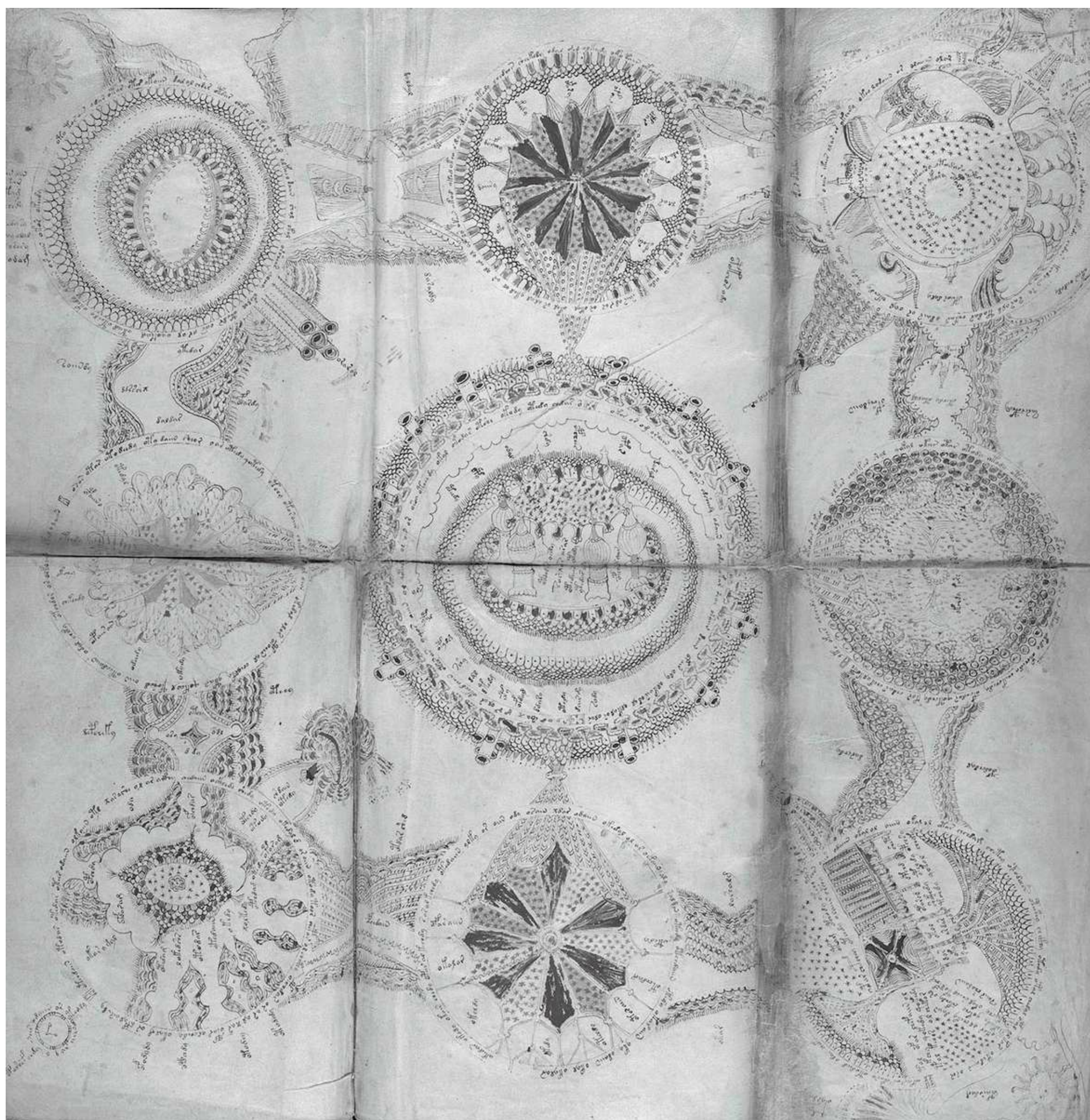


图1-7 手稿的第85v叶及第86r叶（85~86折页全局图）（宇宙学？）

宇宙学部分结束以后，手稿的下一个部分看起来相对容易理解一些。在手稿的这一部分中，我们再次看到了各种各样的植物。但是，这部分的每一页通常会有许多种植物，而不是像手稿一开始的草本/植物学部分那样每页只有一种植物。图1–8展示了这类插图的一个例子。手稿的这一部分通常叫作“药剂学部分”。



图1-8 手稿的第99v叶（药剂学？）

由于图书页面大小的限制，我只能在本书中选择性地复制一小部分手稿中的插图。不过幸运的是，如果读者有兴趣查看手稿的全部内容，这些内容都可以在以下网址找到：http://brbl-dl.library.yale.edu/vufind/Record/3519597。

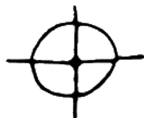
最后，在手稿的末尾还有一个附加部分，这个部分中没有任何插图。因此这个部分被称作“叙述部分”。研究者猜测，这个部分中可能包含一些配方，也有可能是这本书的附录或跋。

当然，对这部手稿的划分方式存在一定的争议。事实上，宾夕法尼亚大学教授威廉·罗曼·纽博尔德（William Romaine Newbold）以及耶鲁大学教授罗伯特·S.布伦博（Robert S.Brumbaugh）都认为本手稿应该被分为5个部分。[注]而其他一些研究者，比如我，则认为这部书稿应该被分为6个部分。[注]假设6个部分的划分方式是正确的，那么我们可以把这本书的6个部分按顺序总结如下：

1. **草本/植物学**
2. **天文学/占星术**
3. **生物学**
4. **宇宙学**
5. **药剂学**
6. **叙述部分（配方？附录？跋？）**

当然，我们不要忘记，还有一种可能是：这些图片事实上与手稿的文字部分毫无关系（虽然这些图片是我们猜测手稿主题内容的唯一初始线索）。

专家的意见



鲁道夫是这样一个人：不管他对什么产生了兴趣，他都会寻求其中最出色的物件。鲁道夫二世的科学藏书涉及范围极广，从天文学到动物学都有所涉猎。鲁道夫二世对天文学的兴趣促成了第谷·布拉赫（Tycho Brahe）和约翰内斯·开普勒（Johannes Kepler）的合作，而这两位科学家最终合作发现了行星的椭圆轨道。此外，鲁道夫二世还建立了一个当时世界一流的艺术收藏库，这个收藏库中包含提香、霍尔拜因、丢勒以及其他艺术家的作品。鲁道夫二世的花园中充满了珍奇的异国花卉，此外他还豢养了很多种野生动物，包括狮子、老虎、花豹、黑豹、熊，以及一只名为奥塔卡的幼狮。有时，鲁道夫二世会允许奥塔卡在门廊里随意走动，这可吓坏了不少宾客。

只要鲁道夫二世想要欣赏世界上各种无与伦比的美物，他就有能力实现自己的愿望。只要鲁道夫二世需要专家的意见，他便能获得专家的意见。在追求知识的道路上，鲁道夫二世不屈不挠，从来不知疲倦。有一次，他为了把铅变成黄金，甚至烧焦了自己的胡子。为了破解这本奇怪手稿中所隐藏的玄妙智慧，鲁道夫二世决定向一位密码学专家求助。但是，在向读者揭示这部手稿的谜底之前，让我们先自己对这本手稿做一番探索和研究。

恺撒的密码



事实上，如果不进行严肃分析的话，这部手稿中的文字本身看起来像是一种极为简单的密码。在这种密码中，每一个字母都被另一个字母取代，进而形成了一个替换系统。为了让这种替换规则容易被记住，尤利乌斯·恺撒制作了一份密码表：每个字母都由该字母后三位的字母来代替。如果我们用现代英文字母表来制作这份密码表，那么在这样一份密码表中，字母A会由字母D来表示，字母B会由字母E来表示，字母C会由字母F来表示，以此类推。当写到字母X的时候，我们就会遇到问题。因为在英文字母表中，字母X后三位的字母不存在了。为了解决这个问题，我们可以回到字母表的开头，循环利用表中的字母，也就是说用字母A来表示字母X。类似地，字母Y可以用字母B来表示，而字母Z可以用字母C来表示。于是，为了方便参照，我们可以把原始字母表（明文）以及密码字母表（密文）以一一对应的方式写成以下的形式：

ABCDEFGHIJKLMNOPQRSTUVWXYZ（明文）

DEFGHIJKLMNOPQRSTUVWXYZABC（密文）

在这种加密方法下，明文信息“THE EVIL THAT MEN DO LIVES AFTER THEM. THE GOOD IS OFT INTERRED WITH THEIR BONES.”[注]经过加密处理以后就变成了以下的信息：“WKH HYLO WKDW PHQ GR OLYHV DIWHU WKHP. WKH JRRG LV RIW LQWHUUHG ZLWK WKHLU ERQHV. ”[注]

有些加密者在做字母替换的时候没有用上面这种非常工整的形式来排列字母。事实上，密码字母表有时可能以随机的形式排布，比如以下这份密码表：

ABCDEFGHIJKLMNOPQRSTUVWXYZ（明文）

JCTBUQAFMOSXWYGDLIVEKRPHZN（密文）

除了上述两种极端情况以外，加密者还可以用一个关键词（或者若干关键词），如“IRON MAIDEN”注来打乱密码字母表的排列。具体如下所示：

ABCDEFGHIJKLMNOPQRSTUVWXYZ（明文）

IRONMADEBCFGHJKLPQSTUVWXYZ（密文）

由于我们不希望把字母A和字母G都被加密为字母I，所以，我们删去了“IRON MAIDEN”中的第二个I，然后再把这个词和原始字母表对齐。出于相同的原因，我们也删去IRON MAIDEN中的第二个N。而不出现在关键词中的字母则按照字母表中的顺序排列。如果我们选择的关键词长度更长，那么字母表会变得更乱。

不管我们使用什么样的字母替换规则，这种编码方式都被称为“单套字母替代式密码”（monoalphabetic substitution cipher）。因为在这种编码方式下，每一个原始字母都由另一个字母来替代，所以把这种加密方式称作“替代式”密码是非常合理的。之所以将这种方式称为“单套”字母替代式密码，是因为在整个加密过程中只用到了一套加密字母表。我们用这种加密方式隐藏原始信息的内容，就像电影中超级英雄用一个面具来隐藏真实身份一样。这种单套字母替代式密码简写为“MASC密码”，以这种加密形式写成的密文被称作“MASC加密文”。

鲁道夫二世所购买的加密手稿使用了一种非常华丽的MASC密码。一般来说，在使用MASC方式加密的时候，加密者会用信息本身所使用的语言的字母表来进行加密。也就是说，基里尔字母密码的明文通常是俄语，而希伯来字母密码的明文通常是希伯来语。

但是，正如上面那些图片所显示的那样，鲁道夫二世所购买的手稿

采用了一套奇怪的字符组合来代表原始明文中的字母。这一变化使得读者更加难以猜出原始明文的内容。我把这套基本字符列于图1–9中。

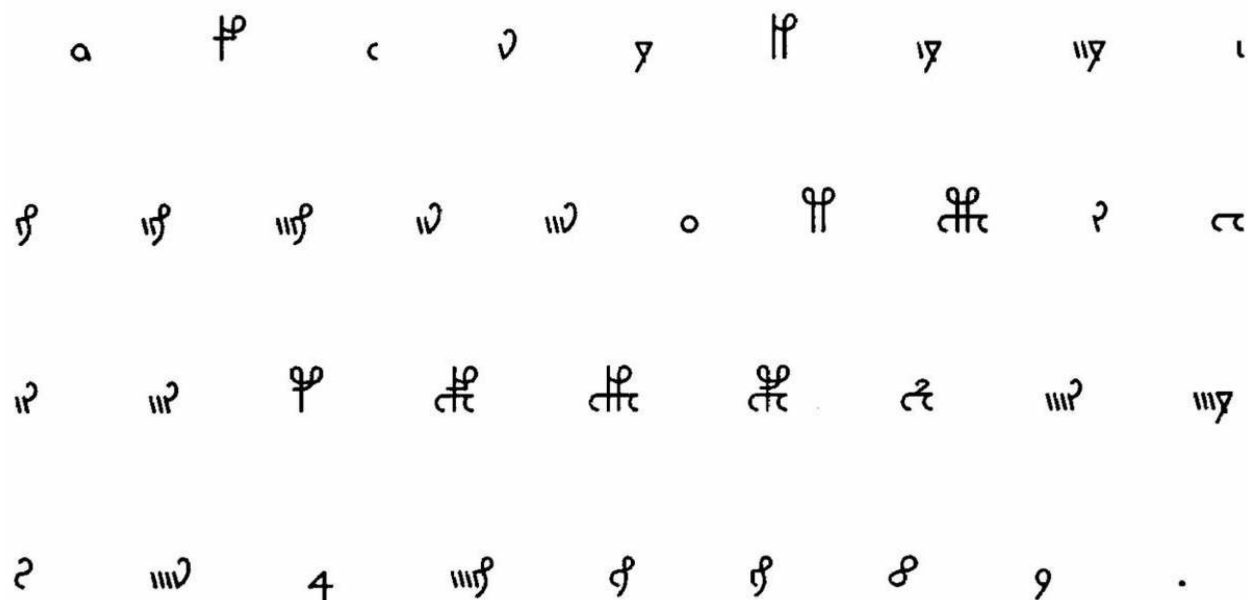
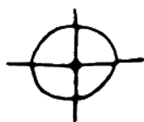


图1-9 基础字符集

如果鲁道夫二世购买的这份手稿中的文字确实是用MASC密码进行加密的话，那么卸下这种伪装应该并不难。但是，在向读者解释破译MASC密码的技术之前，我想先列举一些证据表明上述手稿确实是使用MASC密码进行加密的。我之所以需要证明这一点，是因为即使是在17世纪初，就已经存在许多不同种类的密码加密方式了。

MASC密码的证据



在鲁道夫二世交给密码专家要求其破解的这份手稿中，除了上表中所列出的那些字符以外，还有另一个极为重要的字符，那就是空格！事

实上，在这份200多页的手稿中，空格是出现频率最高的符号。我们不应该把空格的存在视作理所当然，因为在早期的手稿中，作者常常把所有词连在一起书写而不加空格。直到14世纪，欧洲的所有书稿才用空格来把两个词语明确地分开。

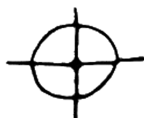
在破译原始信息的过程中，知道每个单词的开始和结束能给破译者提供巨大的帮助。上述信息甚至能帮助我们在开始破译密码之前先确定加密信息究竟是以何种语言写成的。比如说，英语单词的平均长度约为每个单词4.5~5.1个字母。而在德语中，据估计，每个单词的长度约是5.9个字母。德语单词的平均长度之所以超过英语单词，其中的一个原因是：在需要新词语的时候，德语常常会将若干个已有的词语组合在一起形成新词，而不是新发明一个词。根据吉尼斯世界纪录，在目前“仍在使用”的词语中，最长的德语词是Rechtsschutzversicherungsgesellschaften。而在英语中，要表达上述意思则需要用5个单词，即insurance companies providing legal protection（提供法律保护的保险公司）。

在鲁道夫二世的这份手稿中，密文中单词的平均长度在4~5个字母之间。我将在稍后的部分中详细解释，为什么我们没有办法确定地给出一个单词长度的估计值。但是，即使我们只有这个不够精确的词长范围，也足以让我们排除密文是用德语写成的可能性。虽然这样的结论会给我们提供一些帮助，但我们并不能由此立刻确定密文所使用的具体语言（比如英语），因为除了英语之外，还有其他语言的单词平均长度也在这个范围之内。

证明这份手稿是用MASC密码加密的最有力的证据是：在这份手稿中反复出现了一些字母的组合，甚至是完全一样的完整密文单词。如果这份手稿使用的是更加复杂的加密方式，那么我们就应该能看到密文出现更大的变化。在极端情况下，一种理想的加密方式应该能使密文看起来和完全随机的字符串没有任何区别。由于在鲁道夫二世的这份手稿中出现了大量的重复字串，所以我们可以推断出这份手稿使用的加密方式

不可能比MASC密码更加复杂。

如何破解**MASC**密码



如果我们怀疑密文是用MASC密码加密的，那么我们可以用某种语言中的各种不同的规律来尝试破译密文背后的信息。下面我就以英语为例，用一个简单的例子来快速地向读者展示如何用这种方式破解密码。让我们考虑以下这段密文，这段密文背后的明文引自维也纳大公们于1606年拟定的一份协议(注)，这段密文是：

GNX LBURXHW NX NYHRIRXHRD KYJW NY ANPBIDX, BJVGWLNXHX, MBFFBJNXHX BYD HGR JNMR, XSBINYO YK RCSRYXR HK QNYD BJJ MNYDX KQ HIRBXTIRX, JRBIY XRVIRHX BYD TXR XVBYDBJKTX ABWX KQ GBILNYO GNX RYRLNRX ... GR BJXK GBX B AGKJR JNFIBIW KQ LBONV FKKMX. GR XHINERX BJJ HGR HNLR HK RJNLNYBHR OKD VKLSJRHRJW XK HGBH GR LBW NY QTHTIR XRIER B DNQQRIRYH LBXHRI.

要破解这段密文，我们首先需要清点在这份密文中各个字母出现的次数。

A = 3	B = 26	C = 1	D = 9	E = 2
F = 4	G = 12	H = 20	I = 15	J = 16
K = 15	L = 10	M = 4	N = 22	O = 4
P = 1	Q = 7	R = 35	S = 3	T = 5
U = 1	V = 5	W = 7	X = 30	Y = 17
Z = 0				

如果我们把上面列出的各字母出现次数除以这段密文中的总字母数（总字母数= 264），我们就可以得到每一个字母出现的频率，结果如下：

A = 0.011 363 6	B = 0.098 484 8	C = 0.003 787 8
D = 0.034 090 9	E = 0.007 575 7	F = 0.015 151 5
G = 0.045 454 5	H = 0.075 757 5	I = 0.056 818 1
J = 0.060 606	K = 0.056 818 1	L = 0.037 878 7
M = 0.015 151 5	N = 0.083 333 3	O = 0.015 151 5
P = 0.003 787 8	Q = 0.026 515 1	R = 0.132 575 7
S = 0.011 363 6	T = 0.018 939 3	U = 0.003 787 8
V = 0.018 939 3	W = 0.026 515 1	X = 0.113 636 3
Y = 0.064 393 9	Z = 0.000 00	

一般来说，在计算频率的时候使用小数形式比较好。但是，如果你更习惯使用百分比的形式，那么只要把上面列出的所有数字乘以100，

就可以得到每个字母出现频率的百分比。比如，字母R在密文中出现的频率约是13.26%。

接下来，让我们把上述各个字母在密文中出现的频率和正常英语（明文）中各个字母出现的概率(注)进行对比。

表1-1 英语中各个字母的出现概率

字母	出现概率	字母	出现概率
A	0.081 67	N	0.067 49
B	0.014 92	O	0.075 07
C	0.027 82	P	0.019 29
D	0.042 53	Q	0.000 95
E	0.127 02	R	0.059 87
F	0.022 28	S	0.063 27
G	0.020 15	T	0.090 56
H	0.060 94	U	0.027 58
I	0.069 66	V	0.009 78
J	0.001 53	W	0.023 60
K	0.007 72	X	0.001 50
L	0.040 25	Y	0.019 74
M	0.024 06	Z	0.000 74

来源：Beutelspacher，A.，Cryptology（Washington，DC：Mathematical Association of America，1994），10.

从上表中可以看出，在正常英语中，字母E出现的概率最高（字母E是正常英语中最常出现的字母）。而在这段密文中，最常出现的字母是字母R。因此，我们可以暂且假定密文中的字母R代表的是明文中的

字母E。

以上我们检视的只是密文中单个字母的出现频率，我们当然没有必要将视野局限于此。除了单个字母的出现频率以外，我们还可以研究双字母、三字母组合的出现频率，甚至单词的出现频率。在英语中，最常出现的双字母组合是TH，造成这一现象的其中一个原因是：单词“THE”在英语中的出现概率很高。为了寻找单词“THE”的身影，我们可以在密文中搜索出现频率最高的三字母单词。不幸的是，在这段密文中，频率最高的三字母单词有4个。GNX、BYD、HGR和BJJ都分别在这段密文中出现了两次。然而，BJJ的形式和THE不符，因为THE的加密行形式应该包含三个互不相同的字母，所以我们可以据此快速排除BJJ。根据前面的分析，我们怀疑明文字母E在密文中被字母R所取代（因为字母R在密文中出现的频率最高）。而上面的这4种组合中，HGR是唯一一个以字母R结尾的组合，因此，看起来HGR最可能对应于明文中的THE。而作为比较，我们也可以考虑另一种情况，即密文GNX表示明文的THE，那就意味着密文中的字母X代表明文中的字母E（X在密文中出现的频率是0.113 636 3）。还有一种情况是密文BYD表示明文中的THE，那就意味着密文中的字母D代表明文中的字母E，而D出现的频率是0.034 090 9。在后面两种情况中，第二种情况成立的概率实在太低，所以可以排除。但是我们无法排除密文中的字母X代表明文中的字母E这种可能性，因为密文中字母X出现的频率接近于英文中字母E出现的概率，但是，最可能成立的情况仍然是密文中的字母R代表明文中的字母E。通过以上分析，我们可以暂时认为密文中的HGR代表明文中的THE。如果我们把这个结果代入这段密文中，就会得到以下的信息：

```
H      E T       TE E TE                 ,    H    T ,
GNX LBURXHW NX NYHRIRXHRD KYJW NY ANPBIDX, BJVGWLNXHX,
         T      THE    E,             E   E  E T
MBFFBJNXHX BYD HGR JNMR, XSBINYO YK RCSRYXR HK QNYD
              T E    E  ,  E     E  ET         E
BJJ MNYDX KQ HIRBXTIRX, JRBIY XRVIRHX BYD TXR
                    H       H   E E  E ...  HE      H
XVBYDBJKTX ABWX KQ GBILNYO GNX RYRLNRX ... GR BJXK GBX
    H  E                        . HE  T    E      THE
B AGKJR JNFIBIW KQ LBONV FKKMX. GR XHINERX BJJ HGR
T  E  T  E      TE           ETE      TH  T HE
HNLR HK RJNLNYBHR OKD VKLSJRHRJW XK HGBH GR LBW NY
   T  E  E  E       E E T     TE .
QTHTIR XRIER B DNQQRIRYH LBXHRI.
```

虽然目前我们尚无法解读整段信息，但到目前为止的破译结果看上去是合理的。假设当我们把上述字母替换代入整段密文以后得到了EHE或者HHE之类在英语中并不存在的单词，我们就必须后退一步重新尝试其他的字母了。在上面这段被部分破译的信息中，存在一些没有完全拼完的单词（某些字母仍不明确），这就为我们提供了一些进一步破译的可能性。比如，在代入我们假定的三个字母以后，HGBH对应的明文是TH-T：这个单词只缺少第3个字母，我们可以判断这个单词一定是THAT。假设在我们代入某种字母以后，发现某些单词中缺失的字母无论怎么填补都无法形成一个合理的英文单词，那我们就必须后退一步，并重新尝试其他的字母。

现在，我们已经确定密文中的字母B对应于明文中的字母A，因此

我们可以将密文中的所有字母B替换为字母A，然后再次检查是否还有更多容易认出的单词出现。

```
H    A E T      TE E TE            A   , A  H    T ,
GNX LBURXHW NX NYHRIRXHRD KYJW NY ANPBIDX, BJVGWLNXHX,
 A  A   T  A   THE    E,   A         E  E  E T
MBFFBJNXHX BYD HGR JNMR, XSBINYO YK RCSRYXR HK QNYD
A             T EA   E ,  EA    E  ET  A     E
BJJ MNYDX KQ HIRBXTIRX, JRBIY XRVIRHX BYD TXR
  A  A      A      HA      H   E E  E  ... HE A    H
XVBYDBJKTX ABWX KQ GBILNYO GNX RYRLNRX ... GR BJXK GBX
A  H  E     A        A         . HE  T   E  A   THE
B AGKJR JNFIBIW KQ LBONV FKKMX. GR XHINERX BJJ HGR
T  E T  E     ATE          ETE       THAT HE  A
HNLR HK RJNLNYBHR OKD VKLSJRHRJW XK HGBH GR LBW NY
  T  E  E  E A     E E T  A TE .
QTHTIR XRIER B DNQQRIRYH LBXHRI.
```

经过这一步以后，我们的破译结果看起来仍然相当合理。在我们代入了4个替换字母之后，并没有产生任何异常的英文单词。并且我们看到，单字母单词A在密文中出现了两次。破解MASC密码的可能途径有许多种。虽然我们是从单词THE开始入手的，但是另一位解密者可能会首先注意到：在这段密文中，字母B以单词的形式单独出现了两次，因此密文中的字母B只能代表明文中的字母A或I，因为在英语中只有A和I这两个字母可以单独成为单词。

同样，在走到这一步以后，我们继续破译的途径也有不止一条。注

意，在上述半破解的信息中出现了一个以T开头的双字母单词，这个单词一定是TO。在发现了这一点以后，我们就可以确定密文中的字母K代表明文中的字母O。将这一规律代入全文，我们得到以下结果：

```
H    A E T       TE E TE  O          A   , A  H    T ,
GNX LBURXHW NX NYHRIRXHRD KYJW NY ANPBIDX, BJVGWLNXHX,
 A  A   T  A   THE    E,   A      O E  E TO
MBFFBJNXHX BYD HGR JNMR, XSBINYO YK RCSRYXR HK QNYD
A          O  T EA   E ,  EA    E  ET  A     E
BJJ MNYDX KQ HIRBXTIRX, JRBIY XRVIRHX BYD TXR
  A  A O    A   O  HA      H   E E  E  ... HE A  O H
XVBYDBJKTX ABWX KQ GBILNYO GNX RYRLNRX ... GR BJXK GBX
A  HO E      A   O   A     OO  . HE  T   E  A   THE
B AGKJR JNFIBIW KQ LBONV FKKMX. GR XHINERX BJJ HGR
T  E TO E      ATE  O   O   ETE    O THAT HE  A
HNLR HK RJNLNYBHR OKD VKLSJRHRJW XK HGBH GR LBW NY
  T  E  E  E A     E E T  A TE .
QTHTIR XRIER B DNQQRIRYH LBXHRI.
```

在破解这类密码的时候，随着越来越多的字母被破译出来，破译工作的进展也会变得越来越迅速。到了这一步，读者可以随时不再阅读我的分析过程，尝试独立完成接下来的破译工作。

你破解这段密文的途径可能与我的破解途径截然不同。接下来，引起我注意的单词是“A??”，在这个单词中，第2个字母和第3个字母必须是同一个字母。当我顺着字母表走过一遍以后，我发现这个单词有三种

可能性，分别是ADD、ALL以及ASS（请注意这是一段来自1606年的加密信息，因此APP[注]这个组合是不成立的）。事实上，我们没有必要把上述三种可能性一一代入整段密文。我们只需要简单地观察一下这个三字母单词所处的上下文即可。以下哪种情况看起来更合理呢？

ADD THE T--E还是ALL THE T--E还是ASS THE T-- E

虽然我并没有百分之百的把握，但是在我看来上述的第二种情况的可能性最大。我的头脑自动将这段话填补为短语“ALL THE TIME”（所有时间）。当然，我们也可以想象“ADD THE TIME”（加上时间）也是可以成立的，也许这段密文是一段用文字形式表述的数学方程。然而，如果我们把密文中的所有字母J替换为字母D，我们就会发现密文中有其他一些单词没有办法被填补成合理的英文单词。因此，我们通过这种方式又确定了一个之前不知道的字母——L。把这个字母代入整段密文后，我们就可以继续寻找容易认出的单词了。考虑到“ALL THE TIDE”（所有潮水）或者其他一些可能性不大的短语仍然可能成立，在目前这一阶段我们暂时继续保留T--E 的形式。

```
H     A E T         TE E TE  O L          A   , AL H    T,
GNX LBURXHW NX NYHRIRXHRD KYJW NY ANPBIDX, BJVGWLNXHX,
 A  AL  T  A   THE L  E,   A     O E  E  E TO
MBFFBJNXHX BYD HGR JNMR, XSBINYO YK RCSRYXR HK QNYD
ALL       O  T EA   E , LEA     E  ET  A      E
BJJ MNYDX KQ HIRBXTIRX, JRBIY XRVIRHX BYD TXR
  A  ALO    A   O  HA      H   E E  E  ... HE AL O H
XVBYDBJKTX ABWX KQ GBILNYO GNX RYRLNRX ... GR BJXK GBX
A  HOLE L   A   O   A     OO  . HE  T   E  ALL THE
B AGKJR JNFIBIW KQ LBONV FKKMX. GR XHINERX BJJ HGR
T  E TO EL    ATE  O   O  LETEL   O THAT HE  A
HNLR HK RJNLNYBHR OKD VKLSJRHRJW XK HGBH GR LBW NY
  T  E  E  E A     E E T  A TE .
QTHTIR XRIER B DNQQRIRYH LBXHRI.
```

到了这一步，我们可以看出AL-O表示ALSO，而-HOLE表示WHOLE。也许你还能认出其他单词。如果你没有认出来，那么不妨先把新发现的S和W这两个字母代入密文，这样我们也许能获得一些新的启发：

```
H S  A EST   S   TE ESTE  O L    W  A  S, AL H   STS,
GNX LBURXHW NX NYHRIRXHRD KYJW NY ANPBIDX, BJVGWLNXHX,
 A  AL STS A   THE L  E,   A      O E  E SE TO
MBFFBJNXHX BYD HGR JNMR, XSBINYO YK RCSRYXR HK QNYD
ALL     S O  T EAS  ES, LEA   SE  ETS A    SE
BJJ MNYDX KQ HIRBXTIRX, JRBIY XRVIRHX BYD TXR
S A  ALO S WA S O  HA      H S E E  ES ... HE ALSO HAS
XVBYDBJKTX ABWX KQ GBILNYO GNX RYRLNRX ... GR BJXK GBX
A WHOLE L   A   O   A     OO S. HE ST   ES ALL THE
B AGKJR JNFIBIW KQ LBONV FKKMX. GR XHINERX BJJ HGR
T  E TO EL    ATE  O   O  LETEL  SO THAT HE  A
HNLR HK RJNLNYBHR OKD VKLSJRHRJW XK HGBH GR LBW NY
  T  E SE  E A     E E T  ASTE .
QTHTIR XRIER B DNQQRIRYH LBXHRI.
```

到了这一步，我们当然可以继续填补不完整的单词，但是其实我们手中还有一件非常有力的破译工具尚未使用。多年来，各行各业的人不辞辛劳地把各种规模不同的英语词典中的单词根据一些形式进行了分类。一开始，上述工作是靠人工完成的，但是现在计算机程序的发展使得人们可以快速地完成这种分类工作。只要有一张词汇分类表，或者一个计算机运行程序，我们就能够很容易地查找到符合某一特殊形式的英语单词。比如，目前在破译过程中我们有这样一个不完整的单词：-O--LETEL-，我们知道在上述单词中所有缺失的字母都是互不相同的。为了找到这个单词，我们可以求助于一个包含了751 322个英文单词[注]的词汇分类程序。这个程序告诉我们，符合上述形式的英语单词只有一

个，即“COMPLETELY”（“完全地”）。

这样的计算机程序能够帮助我们少费许多力气（这个程序在网络上就能找到，它是完全免费的，并且瞬间就能得到搜索结果）。事实上，我们甚至可以一开始就借助这样的程序。如果密文包含一个形式罕见的单词，也许我们根本不需要知道任何字母，就可以借助这个程序找到这个单词的唯一解法，或者把解法限制在少数几种可能性之中。但是有时候，密文中的每个单词都可能有多种不同的解法，那么在这种情况下，最理想的做法是先分析出若干字母的替换规则，再利用词汇分类表。至此，我们已经找到了字母C、M、P以及Y，接下来让我们继续密文的破译工作：

```
H S MA ESTY  S   TE ESTE  O LY    W  A  S, ALCHYM STS,

GNX LBURXHW NX NYHRIRXHRD KYJW NY ANPBIDX, BJVGWLNXHX,

 A  AL  TS A   THE L  E,   A      O E  E SE TO

MBFFBJNXHX BYD HGR JNMR, XSBINYO YK RCSRYXR HK QNYD

ALL     S O  T EAS  ES, LEA   SEC ETS A    SE

BJJ MNYDX KQ HIRBXTIRX, JRBIY XRVIRHX BYD TXR

SCA  ALO S WAYS O  HA M    H S E EM ES ... HE ALSO HAS

XVBYDBJKTX ABWX KQ GBILNYO GNX RYRLNRX ... GR BJXK GBX

A WHOLE  L   A Y O  MA  C  OO S. HE ST   ES ALL THE

B AGKJR  JNFIBIW KQ LBONV FKKMX. GR XHINERX BJJ HGR

T ME TO EL M  ATE  O  COMPLETELY SO THAT HE MAY

HNLR HK RJNLNYBHR OKD VKLSJRHRJW XK HGBH GR LBW NY

  T  E SE  E A     E E T MASTE .

QTHTIR XRIER B DNQQRIRYH LBXHRI.
```

不管我们手头有没有词汇分类表，我们都很容易看出“H-S　　MA-ESTY”两词显然代表“HIS MAJESTY ”（国王陛下）。当然，我们也可以猜测H-S或许代表“HAS”，但是不要忘记我们已经知道密文中的字母B代表明文中的字母A了，因此这种可能性可以排除。现在，让我们把新发现的字母I和J代入密文中的所有相关位置：

```
HIS MAJESTY IS I TE ESTE  O LY I  WI A  S, ALCHYMISTS,
GNX LBURXHW NX NYHRIRXHRD KYJW NY ANPBIDX, BJVGWLNXHX,
 A  ALISTS A   THE LI E, S A I    O E  E SE TO  I
MBFFBJNXHX BYD HGR JNMR, XSBINYO YK RCSRYXR HK QNYD
SCA  ALO S WAYS O  HA MI   HIS E EMIES ... HE ALSO HAS
XVBYDBJKTX ABWX KQ GBILNYO GNX RYRLNRX ... GR BJXK GBX
A WHOLE LI  A Y O  MA IC  OO S. HE ST I ES ALL THE
B AGKJR JNFIBIW KQ LBONV FKKMX. GR XHINERX BJJ HGR
TIME TO ELIMI ATE  O  COMPLETELY SO THAT HE MAY I
HNLR HK RJNLNYBHR OKD VKLSJRHRJW XK HGBH GR LBW NY
  T  E SE  E A  I  E E T MASTE .
QTHTIR XRIER B DNQQRIRYH LBXHRI.
```

在这段信息中，字母J仅仅出现在MAJESTY一词中，而字母I却多次出现在不同的单词中，因此它可以帮助我们辨认出更多单词。如果你还没有开始尝试自行破解剩余的密码，你可能希望不再阅读我的解答，赶紧独立完成接下来的破译工作了。这段密文的正确解法可以在本章的末尾找到。

以上，我向读者详细介绍了破解一段MASC密码的过程。有了现代计算机的帮助，我们可以更加快速地破解这类密码。事实上，有许多高

级的解法能让我们在几秒钟内破译出上述密码，有时候甚至不足一秒钟。因此，即使我们不知道密码是用何种语言写成的，这个障碍也并不如我们想象的那般巨大。如果一台计算机只需要几秒钟就能破解一种给定语言下的MASC密码，那么即使需要对100种不同的语言进行测试，也不过消耗几百秒的时间而已。当然，根据各种计算机破译程序的性质，程序在每一种语言下会选择不同的词频列表或者词汇分类表。

如果这段密码真的是MASC密码的话，那么鲁道夫二世咨询的任意一位密码专家都能仅使用纸笔破解密码，解决他的问题。然而，事实上，没有一位密码专家解开了鲁道夫二世那份手稿中的谜团。这表明，那份手稿中使用的加密方式并不是简单的MASC密码。

现在，请读者稍事休息，尝试自行破解以下这些MASC密文：

1. PUCM CZODM MUL NLE VSJL OJ HDFOVJ MUL NLYOKF? MUL ZSOXHCIUB ZB LWCKN NCBN UL UCF C “ILKYUCKM JOH ILHWLHNL HLVCMSOKN CKF LHOMSYC.”(注)

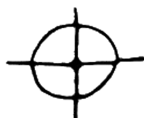
2. JFZ ZSBZMIM INXZ MZSLMEZV, “A ENIU JFLJ A LS VZLV LNV VLSNZV; A LS L SLN BIHHZHHZV QP JFZ VZOAK.”(注)

3. JAAHRMKVW GH EIWIVM, RJOOK EHLI HZ PRJWUI ARIJGIM J WHEIY HUG HZ AEJN GH MIZIVM GXJG AKGN’T CILT JG J GKYI LXIV RUMHEZ LJT KV PHLIR.

4. LDEUCAHE TUZHE’X TEEJ “EHW RZHCUWC XDSBK AUBDM-FWX ALADHXB BRW NABRWNABDMDAHX” PAX CWCDMABWC BE UZCEFI.(注)

5. TUG GOPGFQF AQLCUT QLT TUG ZGAT RI GWGFXTURIC UG EGARFGE. UG GWGI UME URA UQFQAJQPG JMAT ZX IQATFMEMOLA.(注)

浮出水面的证据



前文中，我以密文的平均词长为依据，来证明手稿是用MASC密码加密的。但是，这一统计其实将问题过度简化了。英语中有两个单字母单词，分别是I和A，此外还有许多常用的双字母单词。英语单词的平均词长之所以相对较小，在很大程度上是因为存在上述这些含字母数目较少的单词。虽然我们手头的密文的平均词长符合英语的平均词长指标，但是密文中却鲜少出现只包含一个字母或者两个字母的单词。密文之所以平均词长较低，是因为密文中包含的长单词很少，以及包含大量由4个字母组成的单词。除非它是一份长达200多页的骂文，否则，这份手稿看起来并不是用MASC密码加密的英语文献。事实上，如果我们研究一下这份手稿的词长分布情况，就会发现它并不符合英文的词长分布，也不符合包括拉丁文在内的任何其他欧洲语言的词长分布。然而，如果我们愿意考虑其他可能性，比如这份手稿是用一些更遥远的国家的语言写成的（相对于鲁道夫二世所处的布拉格而言），那么事实上中文、藏文，以及越南文的词长分布情况与该手稿的情况是比较吻合的。㊟

斯拉瓦纳·雷迪（Sravana Reddy）和凯文·奈特（Kevin Knight）将该手稿的部分词频分布与英文（包括含元音和不含元音两种情况）、汉语拼音以及巴克沃尔特转写方案下的阿拉伯语的词频分布进行了比较。结果如图1–10所示。㊟这部分手稿在图中被标记为VMS B，“VMS B”这个名称的具体意义我会在下文中解释。从图1–10中我们可以看出，正常英语（包含元音的英语）的词长分布情况与手稿的词长分布情况最不吻合。如果去除英语中的元音，匹配的吻合度会有所提高，然而，和密文词长分布最为吻合的是巴克沃尔特转写方案下的阿拉伯语。斯拉瓦纳·雷迪和凯文·奈特指出：“从这个例子中我们可以看出，在对密文所使

用的语言得出结论以前，我们应该先把密文与一系列不同的语言进行比较。”注

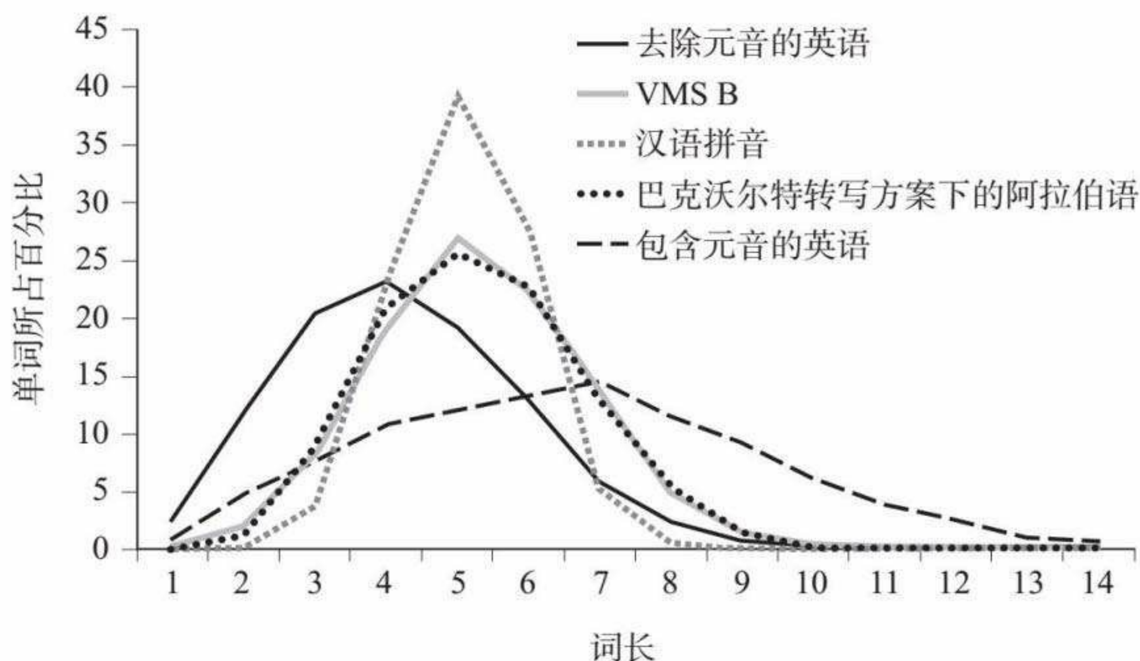
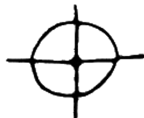


图1-10 几种语言词长分布的比较

幸运的是，统计学并不是我们破解密码的唯一工具，背景信息也能提供不少帮助。具体到这份手稿的情况来看，弄清它的来源或许能帮我们判断出原始信息所使用的语言或是加密的方式，从而大大地推进破译工作的进展。虽然我们手上的信息十分有限，但是鲁道夫二世认为，这段密码应出自罗杰·培根（Roger Bacon）之手，因此我们可以从这点出发。

关于罗杰·培根的猜想



所有秘密都应该用特殊的方式书写下来，以保证粗俗的人无法看懂这些秘密，即使是科学工作者或最热切求知的学生也需要克服重重困难才能破解。只有疯子才会用其他方式来书写秘密。这一点从最开始的时候就已经获得了所有科学工作者的一致认同。通过各种各样的方法，我们成功地将一切科学的秘密隐藏起来，不让粗俗的人获得这些秘密。

——罗杰•培根，《艺术和自然的秘密工作方式，以及魔术的虚空》

（De Secretis Operibus Artis et Naturae, et de Nullitate Magiae, 1252）注

罗杰·培根是一位生活在13世纪的英国僧侣和哲学家。在他之后的几个世纪中，他的声望时高时低。有时候，他被认为是科学实验方法的先驱者，是一位超越了其所处时代的伟人；然而有时候，人们却认为他和同时代的其他所谓的“哲学家”并没有太大区别。

培根懂得很多种语言。据称，他掌握了希腊语、拉丁语、希伯来语、阿拉姆语，甚至一点点阿拉伯语。因此，即使我们假定培根确实是鲁道夫二世购买的这份手稿的作者，我们也无法知道手稿的明文究竟是用什么语言写成的。然而，这样的困难并不能浇灭鲁道夫二世寻找手稿明文的热情，因为培根书写的著作涵盖了科学的各个领域，包括玄学。在《炼金术之镜》（*The Mirror of Alchemy*）一书中，培根向读者介绍了一种丹药的制作方式。他声称，这种丹药不仅可以转化金属，甚至能延长人的寿命。制作这种丹药的正确步骤会不会就隐藏在这份加密的手稿中呢？对于鲁道夫二世而言，获知这一秘密太重要了。

在13世纪，天主教的异端审判法庭已经出现了，因此如果培根想要

书写一份带有异教性质的手稿，他确实有充足的理由要把手稿的内容隐藏在MASC密码背后。然而，即便培根已经采取了这样的预防措施，他的谨慎程度似乎还远远不足以帮他躲避灾祸。事实上，他的各种不加密的异教言论传得满世界都是，比如大家都知道他曾说过“整个神职人员队伍已经变得骄傲、奢侈以及贪婪”，这些言论给他带来了许多负面的关注。[注]因为这些大胆的渎神言论，培根在监狱中度过了14年的时光，在这14年中，他被剥夺了书写的权利。最终，他于1292年出狱，并于同年逝世。[注]几百年之后，一位历史学家声称，在牛津的修道院中，修士们把培根的所有现存手稿钉在墙上，任由它们腐烂。

关于培根的传奇生平，还有许多内容可以讲述。但是对于我们的破译工作而言，这其中最重要的信息是他对密码学的热爱。从本章开头引用的那段话中我们就可以看出，培根极度推崇秘密书写的重要性。然而，鲁道夫二世所拥有的这份手稿似乎采用了一种比MASC密码更为复杂的加密系统，培根有可能使用这样一套加密系统吗？

为了纪念罗杰·培根诞生（大约）700周年，研究者们写了一系列相关论文。在这些论文中，H.W.L.海姆（H.W.L.Hime）中校这样写道：“在《艺术和自然的秘密工作方式，以及魔术的虚空》（后简称《秘密》）一书中，他（培根）花费了巨大的努力，通过密码和字谜的方式来隐藏爆炸物（火药）各个成分的名称和比例。”[注]

我们都知道，早在英格兰人和欧洲大陆人发明火药之前，中国人就已经发现了火药的秘密。然而，中世纪科学与炼金术历史学家林恩·索恩戴克（Lynn Thorndike）甚至都不相信培根是他所处的世界中发现火药的第一人。由于索恩戴克完全否认了海姆的论点，所以这个问题目前仍充满争论。[注]然而，有一个事实是毋庸置疑的，那就是：培根确实曾用密码写过文献。

在本节的开头，我们引用的语句正是来自《秘密》一书。在这本书中，培根描述了7种能够隐藏秘密的书写技巧：

1. “用字符和符号”隐藏信息（比如使用暗号或隐语）。

2. “使用神秘符号或者图形符号”（暗号或隐语）。培根没有清楚地区分头两种方法。他只给出了一个例子，这个例子是哲学家和炼金术士常用的一种暗号。

3. “在书写中只使用辅音”（省略掉所有元音，使阅读变得更加困难）。

4. “把多种字母混合在一起”。有些研究者认为，这条规则指的是使用一些无意义的符号，即在文本中随机加入一些无意义的符号来扰乱读者的阅读，或者把无意义的符号和字母顺序的改变结合起来。然而，培根这样写道：“天文学家艾希克斯（Ethicus）就是用这种方法来隐藏自己的科学知识，他在同一个句子中以希伯来字母、希腊字母，以及拉丁字母进行书写。”根据培根的这种说法，我认为研究者的上述解读是错误的。(注)我认为培根的意思是用不同的方式来书写同一个字母，比如把字母a写作希腊字母α，希伯来字母א，以及拉丁字母a。

5. “使用特殊字母。书写者靠自己的才能和个人意愿创造发明出一些特殊字母，以区别于其他地方使用的字母”（替换）。

6. “不使用字母，而用其他几何形状来代替字母的功能。可以根据点和标记的不同排列方式来代表不同的字母”（替换）。

7. “根据自己的意愿尽量书写得简短一些”（速记）。

在以上7种方法中，第3种方法显得尤其弱。培根这样写道：“希伯来人、迦勒底人、叙利亚人、阿拉伯人用这种方式来书写他们的秘密。”然而，他同时也写道：“但事实上，上述人群几乎用这种通用的方法书写所有内容。”(注)

此外，培根还写道：“我之所以想要描述这些隐藏秘密的方法，是因为我可能会用到上述的部分方法，在我所要书写的秘密非常重要时。通过记录这些方法，我希望至少能在我的能力范围之内为你提供一些帮

助。”㊟

我们可以看出，培根对密码的兴趣已经远远超出了寻常的范围。因此，他可能会在书写一份手稿的时候把上述7种技巧中的几种结合起来使用。但是，我们是否有证据证明鲁道夫二世所购买的这份手稿历史足够悠久，确实有可能是由培根执笔的呢？此外，为什么一份由英国僧侣执笔的手稿最后会出现在布拉格呢？

关于这份手稿在1608年之前的历史，各方研究者提出了各种各样不同的猜测。在20世纪，威尔弗里德·伏尼契（Wilfrid Voynich）成为这份手稿的主人。关于该手稿的历史，伏尼契提出了一种可能的解释，说明了这份手稿是如何从培根手上辗转来到鲁道夫二世的宫廷中的。当然，伏尼契先生显然希望这份手稿的作者是培根，而不是某个不知名的作者，因为只要能证明这一点，就能够提高他所拥有的这份手稿的价值。虽然现存的证据不足以确证这份手稿的作者确为培根，但是我在此仍列出这种可能性供读者参考。

根据伏尼契的说法，培根于13世纪后半叶完成了这份手稿，然后这份手稿就一直被收藏在英格兰某所修道院的图书馆中，直到1538年。这个故事的开头似乎一点儿也不激动人心，但是请读者不要着急，我们只需要一句话，就能轻而易举地把这份手稿和鲁道夫二世联系起来。接下来，在宗教改革的混乱中，该修道院解体，诺森伯兰公爵约翰·达德利（John Dudley）借此机会夺取了这份手稿。众所周知，达德利从教会及其他宗教机构处获得了不少战利品，但是这份手稿是这些战利品的其中之一则纯属猜测。如果以上的猜测属实的话，那么有可能约翰·迪伊（John Dee）于1547年从达德利手中获得了这份手稿。

虽然我们并不知道迪伊是否曾经拥有过我们所讨论的这份神秘的手稿，但是我们知道他确实曾经拥有过大量培根的手稿。迪伊购买了他能找到的所有培根的手稿。事实上，正是因为迪伊的努力，人们才对培根的那些几乎被遗忘的作品重新产生了兴趣。为了寻找培根的手稿，迪伊走遍了整个英格兰，终于建立起一座图书数量相当可观的收藏馆，这也

是当时整个英格兰最大的私人图书馆——“藏书总量近4 000册”。在收集这些图书的过程中，为了节约资金，迪伊有时会向别人借阅书籍，然后适时地“忘记”归还。

根据猜测，这份手稿于1584—1588年之间被迪伊从英格兰带到了布拉格，鲁道夫二世以600个达克特金币的价格从迪伊手中购买了这份手稿。至此，这份手稿假想中的流传轨迹画上了句号。在稍后的部分中，我们将进一步研究支持这次交易的证据。伏尼契认为，迪伊把这份手稿当作“礼物”赠送给了鲁道夫二世。

关于这种猜测，我们有若干细碎的证据，有的支持这种猜测，有的则不支持。

证据1（不支持）：如果这份手稿确实为罗杰·培根所作，那么这份手稿的成书日期就应早于哥伦布。如果是这样的话，这份手稿如何能够包含一幅描绘向日葵的插图呢？（见本章之前提到的该书第33v叶。）我们知道，向日葵是一种原本生长于美洲的植物。直到1493年，哥伦布才首次将向日葵的种子带回欧洲。当然，不相信这一证据的人可以声称，该插图中描绘的植物其实并不是一株向日葵。（还记得这株植物奇怪的根系结构吗？）或者，他们也可以说，绘制这幅插图的人从某些早于哥伦布访问美洲的人那里了解到了向日葵的样子（维京人？中国人？），虽然这种说法比较牵强。

证据2（支持？）：某些专家，比如《约翰·迪伊藏书目录》的编辑之一安德鲁·G.华生（Andrew G.Watson）教授声称，这份手稿上的页码和迪伊的字迹相吻合。[注]当然，也有一些专家反对上述论点，拉法乌·普林克（Rafat Prinke）认为，手稿页码中的“8”显然不是迪伊的笔迹。普林克还提出了更多细微的笔迹上的区别，其他专家也提出了一些[注]。我们知道，迪伊喜欢把自己的名字或者代表所有权的标志写在他的藏书上，还喜欢在自己的藏书上做页边批注，但我们在这份手稿中并没有发现上述这些痕迹。

证据3（支持）：迪伊对密码学很有兴趣。他曾评价另一本与密

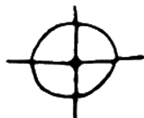
码学有关的书《隐写术》（Steganographia）是比“一千顶皇冠”还值钱的“最珍贵的珠宝”。许多有权势的人都了解迪伊对密码学的兴趣，比如弗朗西斯·沃尔辛厄姆爵士（Sir Francis Walsingham）就曾经为了获得更多密码学方面的知识而拜访迪伊。注

证据4（支持？）：迪伊的儿子阿瑟说过，自己的父亲曾花费很长时间研究一本“除了象形符号以外什么也没有的书”。注虽然有些人可能会觉得这只是阿瑟不经意间使用了一个不同的表达，但是事实上这份手稿中的内容看起来更像某种奇怪的手书体，而并不像象形符号。此外，这份手稿中虽然有一些书页只有文字没有插图，但大部分书页都配有大幅的彩色插图。因此把这样一份手稿描述为一本“除了象形符号以外什么也没有的书”，事实上并不准确。

证据5（支持）：在1584—1588年间，迪伊确实数次去过鲁道夫二世的宫廷。但是我们并没有任何证据证明在这几次访问中迪伊向鲁道夫二世出售过这份加密的手稿。

正如我在前文中指出的，伏尼契提出的这种假说是有可能成立的，但是由于没有充分的证据，这一假说与真实情况未必相符。

这会是一个骗局吗？



鲁道夫二世的身边充满了各种各样的炼金术士，也许有些人真的相信自己所从事的炼金事业，他们可能真的相信自己正在逐步获得点石成

金的秘密。就算是备受尊敬的人类历史上最伟大的科学家艾萨克·牛顿爵士，也曾经在炼金术领域花费了相当多的时间，比花在令他成名的科学研究领域的时间还要多。然而，也有许多炼金术士并不真心相信炼金术，纯粹是在用各种各样的戏法招摇撞骗。其中一种戏法是在空的勺子里放上金子，然后再用蜡封住。他们用这种做过手脚的勺子在锅里搅拌，勺子上的蜡就会逐渐融化，于是锅里就出现了金子，看上去就像是用锅煮出了金子一样。迪伊的朋友爱德华·凯利（Edward Kelley）则喜欢使用另一种障眼法，迪伊也有份。这种戏法会用到一种双层底的坩埚，坩埚中也同样藏有金子，并用蜡封住，当蜡融化时，所谓的“炼金术”也就成功了。当然，还存在许多比上述两种戏法更为复杂的障眼法。对那些愿意相信炼金术的人而言，很容易把上面的这些戏法当作炼金术成功的证据。

我们要回答的问题是：如果鲁道夫二世会被这些虚假的“化学实验”愚弄而甘愿献出自己的部分财富，那么他是不是也有可能被一本其实毫无意义的手稿愚弄呢？鲁道夫二世购买的这份奇怪手稿上记录的会不会只是一个虚假字母表中的随机字符呢？作者为了创造这份手稿而花费的努力真的有价值吗？毕竟这份手稿的长度有200多页……

在前文中我们已经提过，据称鲁道夫二世花费了600个达克特金币来购买这份手稿，因为他相信这份手稿有可能帮助他实现自己的目标。当时600个达克特金币的价值相当于今天的100 000美元。因此，我们有理由相信，在这种巨大的经济利益的诱惑下，肯定有人愿意花费时间来制造一份手稿。

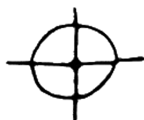
迪伊可不会觉得这样的骗局有失自己的身份。事实上，这份手稿完全有可能是迪伊自己制造出来的（下面我还会进一步讨论这个问题）。迪伊的另一重身份是一名间谍，在他所处的时代中，间谍被认为是一种非常不体面的职业。直到最近，这种职业才因为詹姆斯·邦德等影视形象的出现而带上了光环［事实上间谍这份职业的光环的产生或许可以追溯到詹姆斯·费尼莫尔（James Fenimore）于1821年出版的小说《间谍》

（*The Spy*）］。迪伊在炼金术方面的冒险故事至今仍被人们所熟知，甚至有一幅19世纪的画就叫作《约翰·迪伊为鲁道夫二世表演炼金术》。因此，我们有充分的理由相信，只要有利可图，迪伊绝对乐于用各种方式误导他人。

不管怎么说，鲁道夫二世招来的各位行骗高手之间显然存在着激烈的竞争。事实上，迪伊也曾被他的朋友爱德华·凯利骗过。凯利曾经告诉迪伊，自己能与天使交流。凯利还声称，天使告诉他，上帝要求迪伊和他共享妻子。而迪伊真的相信了凯利的说法。

后来，迪伊的这种生活方式终于给他带来了麻烦，最终，他不得不从鲁道夫二世身边逃离。在迪伊逃离期间，他的图书收藏馆丢失了500本书。而和迪伊一样过着骗子和间谍的双重危险生活的凯利当时则比迪伊运气好，他靠着这些手段获得了爵士的封号。注不过，最后凯利也和迪伊一样下场悲惨，他被鲁道夫二世投入地牢，饱受折磨。凯利曾试图从鲁道夫二世的地牢中逃跑，然而他的越狱计划进行得并不顺利。凯利因为试图越狱受到酷刑的惩罚，最终重伤而死。

其他可能性



我们应该记住：就算这份神秘的手稿不是为了行骗而伪造的，它仍然可能毫无意义。也许这份手稿的作者有精神疾病，或者是在药物的影响下写出了这份手稿，也有可能作者当时正受到周期性偏头痛的折磨，或者处于宗教上的狂喜状态。在上述这些情况中，即便作者并不想欺骗任何人，他也仍然可以写出一份毫无意义的手稿。也许，之后有人发现了这份手稿，却并不知道上面的情况，于是便把这份毫无意义的手稿当

作加密的文件。布伦博曾用这样的语句描述该手稿的插画作者：“他把植物看作了活化的东西，这种状态已经在精神错乱的边缘上了。”[注]然而，如果我们把这份手稿的内容和一些真正的精神病人的作品进行比较，就会发现两者之间也并不具有很高的相似度。

另一种可能性是，这份手稿只是一件艺术品。看起来像加密手稿的艺术品是确实存在的。路易吉·塞拉菲尼（Luigi Serafini）1981年创作的《塞拉菲尼抄本》（*Codex Seraphinianus*）就是一个例子。从《塞拉菲尼抄本》中的插图我们可以看出，《塞拉菲尼抄本》是一本百科全书式的书，其涵盖的主题范围甚至比我们讨论的这份奇怪的手稿更宽泛。虽然《塞拉菲尼抄本》的内容本身没有任何意义，但我们却可以把它当作一种超现实主义的艺术品来欣赏。在《塞拉菲尼抄本》中，文字中穿插着各种奇异的图，这些文字粗看上去像是用一种独特的字符写成的加密文字。我们并不清楚《塞拉菲尼抄本》中的文字是否只是乱写的，但有人判断《塞拉菲尼抄本》中的页码是用一种类似密码的加密方式标注的。[注]

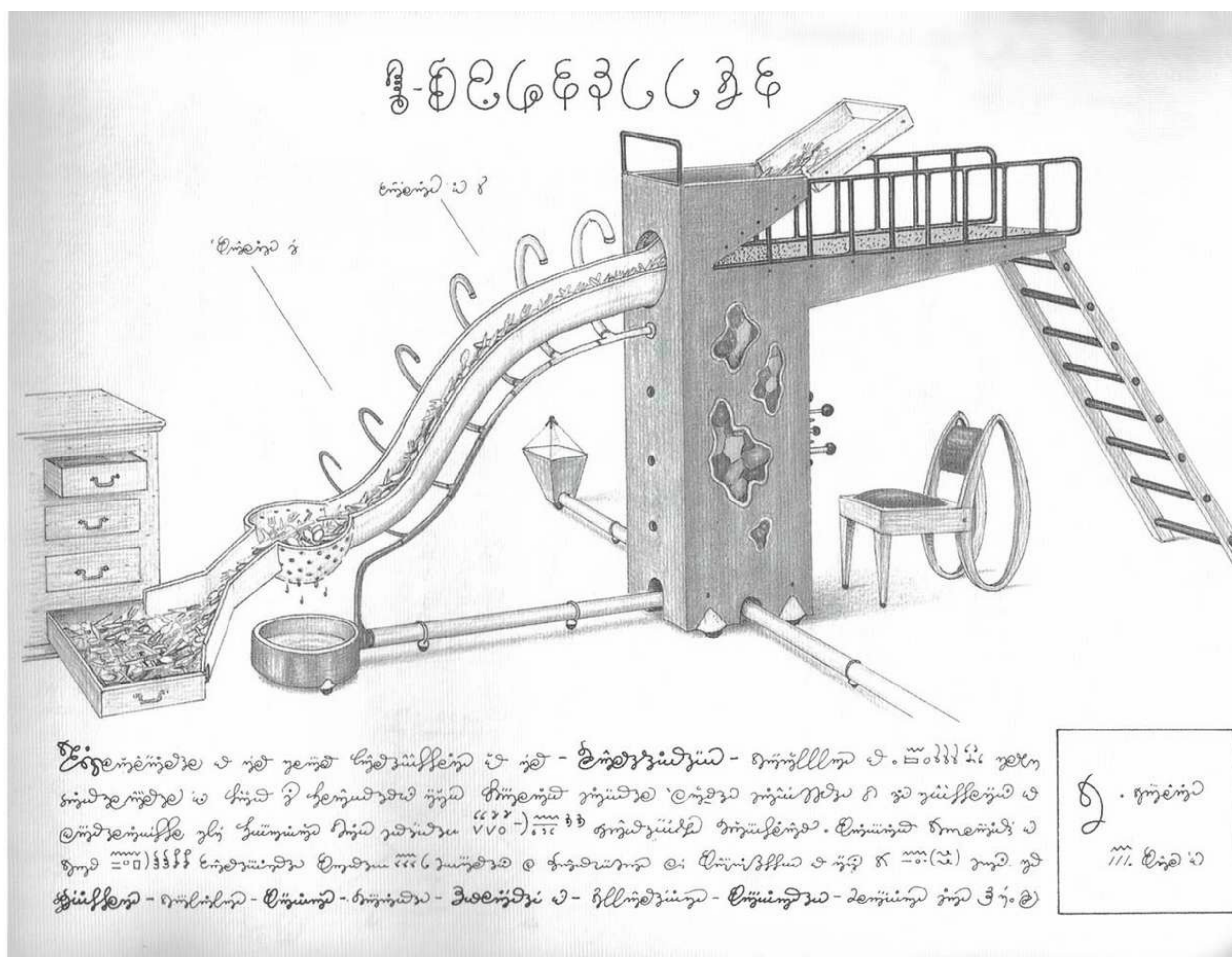
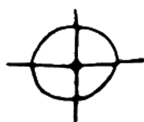


图1-11 《塞拉菲尼抄本》中随机选取的一页

鲁道夫二世的努力



没有任何证据显示鲁道夫二世曾考虑过这份手稿只是一个骗局。事实上，要是鲁道夫二世认为这份手稿纯属伪造，那么我们也许就会听到另一个关于凯利如何被无情的命运所惩罚的传奇故事了。要是鲁道夫二

世觉得被骗了600个达克特金币，他可不会心慈手软！相反，据我们所知，和鲁道夫二世关系密切的各路专家用各种方法不断试图为鲁道夫二世解开这份手稿的秘密。

在前文中，我们猜测过这份神秘手稿在落入鲁道夫二世手中之前的历史，但在手稿到了鲁道夫二世手中后的阶段，我们就有一些确凿的事实证据了。在讲述这段历史的时候，我们不妨从特潘内兹的雅各布斯·霍尔契奇（Jacobus Horcicky de Tepenecz）说起。他是鲁道夫二世的首席植物学家和药剂师，负责管理鲁道夫二世的皇家花园。霍尔契奇最大的贡献在于他发现了把花的香味转化成液体的方法。也就是说，他发明了香水。在“特潘内兹的雅各布斯·霍尔契奇”这个名字中，“特潘内兹”是他因为在1608年靠药剂救了鲁道夫二世的性命而获得的贵族封号。由于这份神秘手稿中含有大量的植物图，所以鲁道夫二世在选择破译该手稿的人选时，很可能一开始就会想到霍尔契奇，这种猜测是非常合理的。


IACOBUS HORZICKY
Clemens Kohl sc: Viennæ

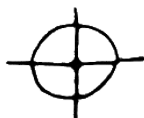
图1-12 特潘内兹的雅各布斯•霍尔契奇（1575—1622）

霍尔契奇与这份手稿之间的联系很长时间以来一直不为人所知，直到后来一位所有者试图用影印的方式复制这份手稿的第一页时，才意外地发现了霍尔契奇与这份手稿的联系。当此人影印该手稿的第一页时，由于曝光不足，该书第一页下方的一个已经褪色的签名显现了出来。在给原本涂上化学物质以后，这个签名更加清晰地显示了出来。这个签名的存在似乎显示霍尔契奇是这份手稿的主人。因为如果这份手稿属于鲁道夫二世，并且鲁道夫二世只是把这份手稿暂时借给霍尔契奇破译的话，那么为什么霍尔契奇要将自己的名字写在手稿的书页上呢？当你向别人借书的时候，你当然不会在别人的书上写上你自己的名字，除非你像迪伊一样根本不打算归还！

霍尔契奇的签名中包含了“特潘内兹”这个封号，因此我们知道，他是在1608年以后的某个时间拥有这份手稿的。此外，在他自己的名字下面还写有“布拉格”（“Prag”）一词。我们知道霍尔契奇于1618年离开了这座城市，因此写下该签名的时间应该早于1618年。

身为鲁道夫二世的宠臣虽然是一件很有价值的事情，但这种价值持续的时间并不太久。后来，鲁道夫二世失势，被他的弟弟马蒂亚斯（Matthias）取代——但鲁道夫二世一直在名义上保持着神圣罗马帝国皇帝的称号，直到他1612年去世。因此我们知道，即便这份手稿中真的写有长生不老的秘密，这个秘密显然未能被及时解开，也显然没有帮助鲁道夫二世获得永生。因此，一种比较合理的解释是，霍尔契奇可能在鲁道夫二世最后的日子里获得了这份手稿的所有权，或者是在鲁道夫二世死后不久。1618年，布拉格被新教徒控制，主管与布拉格邻近的梅尔尼克地区的天主教徒霍尔契奇被投入了监狱。然而，上天又一次眷顾了霍尔契奇，在斐迪南大公胜利后，天主教重新控制了布拉格。霍尔契奇最终死于1622年的一次骑马事故。

格奥尔格·巴雷什



在霍尔契奇死后，这份手稿又落入了何人手中？针对这个问题，存在各种各样的猜测，但是我们并没有确凿的证据来证明任何一种猜测。下一个被确认的主人是格奥尔格·巴雷什（Georg Barsch），又名乔治·巴修斯（Georgius Barschius）。在霍尔契奇和巴雷什之间，这份手稿可能有过一名或多名主人。我们之所以知道巴雷什是这份神秘手稿的主人，是因为在罗马的宗座额我略大学（Pontificia Università Gregoriana）的档案馆中发现了一封书信。[注]这封书信由M.J.戈尔曼（M.J.Gorman）誊抄，于2010年由斯莫尔卡（Smolka）和赞德伯根（Zandbergen）出版。这封信全文如下。巴雷什之所以在信中对阿塔纳修斯·基歇尔（Athanasius Kircher）大加赞美，是因为他认为基歇尔是一位伟大的语言学家。基歇尔写过一本关于科普特语的书，这是一种生活在埃及的早期基督徒们所说的语言。许多人相信，解开埃及象形文字含义的人可能就是基歇尔——在当时，没有任何人能够理解埃及象形文字的含义。

乔治·巴修斯写给阿塔纳修斯·基歇尔的信（1639）[注]

最尊敬的神父，

希望我的这封信不要过分地打搅您。在此我祈祷上帝将所有快乐赐予尊贵的您。

因为一位神职人员即将启程前往意大利和罗马，所以我决定抓住这个机会请他将这封信转交给您。我曾托布拉格耶稣会的一位牧师——尊敬的莫雷特斯神父转交给了您一份文稿，希望这封信能唤

醒您对那份文稿的回忆。

您通过出版《科普特语简史》（Prodromus Copticus）一书赢得了国际声誉。在这本书中，您曾经呼吁任何持有相关材料的人将这些材料呈送给您，因为这样可以帮助您增加手中的相关资源，进一步丰富您的著作，并使您的研究成果更加成熟。

我相信，在您发出这一呼吁以后，人们一定已经将大批材料送到了罗马。这其中有许多人一定是亲自把手中的材料送到您面前的，这样做是为了表达对您的敬意，因为您在语言方面做出了卓越的努力，并且付出了超乎常人的辛劳。当我听说这个振奋人心的消息时，告诉我消息的人也向我展示了一本惊世杰作的简要提纲，我相信这本伟大的著作将会在我们的时代重见天日（而且我认为事不宜迟）。向我提供消息的人还告诉我，您在解开一些极为晦涩的手稿中隐藏的谜题这方面也有着出众的能力。

在我的个人图书馆中，有一份用未知文字写成的手稿，这份手稿就像是斯芬克斯的谜题，它在我的图书馆中没有任何用处，只是徒然占据空间。因此，我想把这样一份谜题送给“埃及的俄狄浦斯”[注]进行破解应该不能算是不当之举。所以，我派人将这本古老的书的一部分重新誊写，并保证字迹尽量忠实地模仿原文（将这封信呈送给您的人将向您证实他亲眼见证了这一点）。一年半以前，我也将这份誊抄过的手稿送交给了最尊敬的您。如果您认为合适的话，我希望您能拨出一些宝贵的工作时间来研究这份手稿，并将手稿中那些未知的文字破译为我们能够阅读的字符。如果这份手稿所隐藏的秘密承蒙一位像您这样的一流学者花费宝贵精力的话，那么我希望我的这一举动既能够为该手稿解谜者和我自己带来一些益处，也能够为公众做出贡献。

由于您与我之间的这段旅程既漫长又危险，我认为让这部手稿的原件经历这些危险是不明智的。而且经过了漫长的等待以后，我一直没有收到您的回复，因此我只能认为此前的那份手稿并没有到达罗马，也没有到达您的手中。所以，我决定再次将这份手稿的誊抄版呈送给您。当上文提到的莫雷特斯神父告诉我，他已经把这份

手稿带到了罗马的时候，我感到万分欣喜。如果尊敬的您愿意解开这份手稿的秘密，让所有有识之士共同拥有这本书中埋藏的宝藏，那么我必将感到更加欣喜。

这本书中包含大量的植物图，还有许多描绘星星的图，以及其他带有化学符号的图。根据这些信息，我个人猜测，这部手稿的主题可能与医学相关，而医学是除了救赎灵魂的神学以外最能够惠及整个人类的研究领域。破解这份手稿中的谜题并不会伤及像您这样一位伟大智者的尊贵身份。既然作者如此谨慎地对手稿进行了加密处理，显然他并不希望未受过教育的无知民众了解手稿的内容。事实上，我们很容易设想，某位有识之士为了寻找真正的医药而亲自寻访了东方世界（因为他发现欧洲所流行的医药并不具有很高的价值）。也许，这位有识之士通过研读文献以及与当地的医疗专家交流而获取了埃及医药知识的宝藏，他将这笔宝贵的财富带回欧洲，并将这些知识藏在了这部书稿中。这本书中包含许多在德国从未有人见过的异域植物图，这使我对上面的假说更加深信不疑了。

我相信最尊敬的您对让最宝贵的东西重见天日一定有极大的热情。如果能把这本手稿中隐藏在未知字符下的宝藏挖掘出来（如果这本书中真的埋藏有这种宝藏的话），就能为公众做出贡献，因此我希望您不会认为这样一份解谜的工作有失您的身份。事实上，我认为任何人都没有能力完成上述工作，因为这份极为晦涩的手稿中的秘密需要独特的智慧和敏捷的思维，或是一种显然无法轻易掌握的新方法才能够解开。这份手稿中也许藏有巨大的宝藏，解开这份手稿的秘密也许会使许多从前不可能的事情变成可能。因此，如果您愿意进行这项工作，我将感激不尽。为了唤醒您的记忆，我将在此附上这份未解手稿的两行内容，之前我已经向您呈送了用类似字符写成的整部手稿。

希望我的这封信能给您留下良好的印象，同时也预祝您崇高的努力能够获得圆满的结果。愿最伟大和最完美的上帝为了语言学领域的福祉保佑您长寿。

公元1639年4月27日于布拉格，在这一天我走进了罗马的智慧学

府，并为人类的医学智慧做出了我自己的贡献。

向尊敬的您致以最高的敬意

乔治·巴雷什先生

在上面的这封信中，巴雷什提到他之前曾经给基歇尔写过另外一封信，但是前一封信已经丢失。此外，关于这些书信的作者的生平信息也已经无迹可寻。我们从未发现基歇尔给巴雷什的回信，甚至没有证据显示基歇尔对这封书信做出了回复。但是我们却知道这份神秘手稿的下一任主人是谁。巴雷什于1662年去世，他将包括这份加密手稿在内的所有藏书留给了兰什克龙的约翰内斯·马库斯·马尔奇（Johannes Marcus Marci of Kronland）。

在马尔奇生活的年代，一个人仍然可能在若干不同的领域中同时取得较高的成就。马尔奇不仅是一名医生，还是一位颇有名望的数学家、物理学家以及东方学家。他曾担任过布拉格大学的校长。


IOANNES MARCVS MARCI PHIL: & MEDIC: DOCTOR
et Professor natus Landscronæ Hermundurorum in Boemia
anno 1595. 13 Iunij.

图1-13 约翰内斯•马库斯•马尔奇（1595—1667）

我们不清楚马尔奇究竟花了多长时间试图破译这份神秘的手稿。但我们知道，在马尔奇的生命走向尽头时，他把这份手稿寄给了一位比他声望更高的知识分子，此人就是罗马的阿塔纳修斯·基歇尔，与此前巴雷什写信求助的基歇尔是同一个人。几个世纪以后，这份手稿以及随手稿同时寄出的马尔奇写给基歇尔的书信被同时发现。事实上，关于这份手稿来源的信息很大一部分都是出自马尔奇写给基歇尔的那封书信。这封书信全文如下[注]：

尊敬而高贵的先生，亲爱的神父：

这本书是我的一位亲密的朋友赠予我的。从拥有这本书开始，我就认为我应该把这本书交给您，我亲爱的阿塔纳修斯，因为我一直相信除了您以外，没有人能够读懂这本书稿。

这本书的前任主人曾经去信询问您的意见，他还誊抄了这本书的部分内容随信寄送给您。他相信，只要看到这本书的部分内容的誊抄本，您就能了解剩下的内容，但当时他并不愿意将所有原稿寄给您。为了解开这部手稿的密码，这本书的前任主人付出了不懈的艰苦努力，在此我将他已有的一些材料随信寄给您。通过这些材料，您一定可以清楚地看到他的努力。直到生命的终结，这部书的前任主人才最终放弃了破译这部手稿的希望。然而，事实证明，他的一切努力都只是白费，因为像这样的斯芬克斯只会服从命定的主人，也就是您，基歇尔。现在，请接纳这部书稿的原件吧，同时也请接受我对您的敬爱之情，虽然我早就应该向您表达我的感情。希望您能够成功克服这个谜题带来的困难——如果说这个谜题对您来讲还有什么困难的话。希望您能像过去一样取得巨大的成功。

拉斐尔博士[注]曾任斐迪南三世的波希米亚语教师，而斐迪南三世日后成为波希米亚的国王。拉斐尔博士告诉我，上文提到的这部书稿曾经属于鲁道夫二世，他还告诉我，鲁道夫二世曾花600个达克

特金币从前任主人手中买下了这部书稿。他相信这部手稿的作者是英国人罗杰·培根。关于这一点，我保留意见。希望您能够告诉我们究竟应该如何看待这部书稿。为了报答您对我的善意和恩惠，我将永远毫无保留地把自己奉献给您。

听候尊敬的您的调遣，
兰什克龙的约翰内斯·马库斯·马尔奇
布拉格，1665年4月19日

（信件原件所署的年份也可能不是1665年，而是1666年。因为原件中年份的最后一个数字很难看清楚。）

上述这封书信提出了这样一个谜题：在“这本书的前任主人曾经去信询问您的意见”一句中，所谓的“前任主人”究竟是谁？在若干个世纪的时间中，这个谜题一直未被解开。正如我们在前文中已经提到的，现在我们知道，这位“前任主人”就是格奥尔格·巴雷什。

现在，让我们来谈一谈阿塔纳修斯·基歇尔。似乎没有什么领域是基歇尔不感兴趣的。在他的著作《知识的伟大艺术，或者组合艺术》（*Ars Magna Sciendi Sive Combinatoria*）一书的扉页上，基歇尔写道：“没有什么东西比知晓一切更加美妙了。”这句话似乎也是他的人生目标。在基歇尔的一生中，他惊人地在不同领域中做出了各种各样的贡献。他的著作超过40本，这些著作的主题范围极为广泛，包括中国书法、巴洛克音乐、宇宙学、化石、地质学、魔法灯笼、磁学、凤梨（基歇尔认为这种异域水果可以吞噬铁钉），以及地下世界。为了追求知识，基歇尔甚至不惜冒生命的风险。为了获得关于火山的直接经验，他曾经亲自深入维苏威火山炽热的火山口中。从基歇尔的描述中我们可以看出，即使只是站在火山口的上方就已经够可怕的了：


IHS P. ATHANASIUS KIRCHERUS FULDENSIS E SOCIETATE IESU ANNO ÆTATIS LXII ANNO CIↃ IↃ C LXIV.
Frustrà vel Pictor, vel Vates dixerit, HIC EST:
Et vultum, et nomen terra scit Antipodum.
Jacobus Albanus Ghibbesius, M.D.
in Rom: Sapientia Eloq: Prof.

图1-14 阿塔纳修斯•基歇尔（1602—1680）

> 我想地狱也不过如此。除了可怕的幻影和魔鬼的幽灵，地狱里的一切那里都有。在那里，我听到山发出恐怖的吼叫，我闻到一种无法描述的恶臭。烟雾混合着暗色的火球，从火山底部和侧面大约11个地方不断喷射出来。面对这样的情景，我也像火山一样开始打嗝和呕吐。[注]

除了撰写他自己的著作以外，基歇尔还汇编其他人的报告，比如从远东归来的耶稣会传教团的报告。基歇尔甚至早于达尔文提出了动物物种会发生进化的理论。

从这份神秘手稿的插图中我们可以看出，这部手稿涵盖了范围极广的各种内容。既然基歇尔的知识和兴趣也涉及非常广泛的领域，他的广博学识也许会赋予他着手研究和破译这份神秘手稿的自信。基歇尔一定非常希望获得这份加密手稿中隐藏的知识，而现在他已经拥有了这份手稿。正如我们在前文中看到的，不管是巴雷什还是马尔奇都认为，最有可能破解这份加密手稿的人就是基歇尔。除了上面提到的这些能力以外，基歇尔还拥有一些特殊的知识和技能，使得他有潜质成为一名优秀的密码破译者。

基歇尔的职业是罗马大学的一名数学教授。数学家可以成为非常优秀的密码破译专家——虽然人们直到第二次世界大战才认识到这一点。在基歇尔的各种数学著作中，有一部分著作的内容属于组合论的领域。在当时，组合论研究的主要内容是从一个有限集合中找出可能的元素组合。在理想的状态下，数学家不应该通过穷举所有可能性来得出可能组合的总数。也就是说，数学家应找到某种计算组合总数的捷径。基歇尔画出了可能是世界上第一张完整的二分图：图中的点被分为两组，第一组中的每一点都和第二组中的每一点以一条线连接。图中的线段总数就是从两组中各选出一个元素所能得到的组合数目。此外，基歇尔还发明了一套逻辑系统。

1663年，基歇尔在《组合艺术所揭示的一种多语言适用的全新通用书写方法》（*Polygraphia Nova et Universalis ex Combinatoria Arte Detecta*）中直接讨论了密码学的问题。该书中有一些基歇尔的原创贡献，但是大部分是其他人已经提出的内容，包括一些比我们前文讨论过的MASC密码更加复杂的加密系统。这本书中最重要的是介绍了一种“通用书写符号”（pasigraphy）系统。发明这种系统的目的是创造一种人工语言，既容易学习，又可以表达复杂的含义。有了这样一种通用书写系统，人类就能够通过这种语言进行交流。在基歇尔的这套系统中，他用数字代替了我们习惯使用的文字，因此这一系统只能被用于书面交流，而不能用于口头交流。其他一些晚于基歇尔的系统，如1887年发明的世界语，则创造出了一种通用的“语言”——既能满足书面交流的需求，也能满足口头交流的需求。

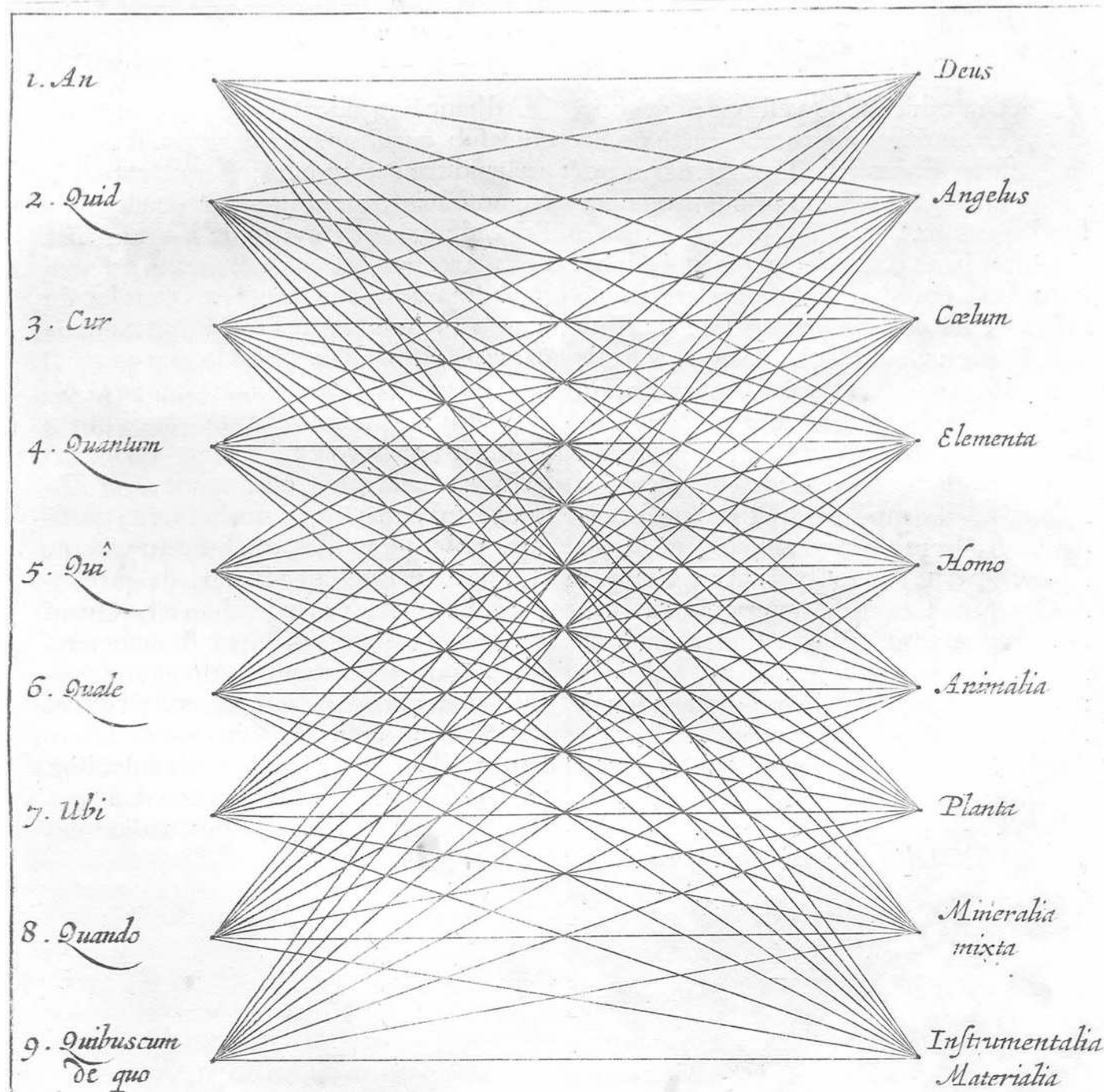


图1-15 一幅完整的二分图，该图摘自《知识的伟大艺术，或者组合艺术》

除了上述这些成就以外，我们在前文还提到，基歇尔是一名伟大的语言学家，人们期待着他能破解古埃及象形文字的秘密。因此，马尔奇才会在写给基歇尔的书信中提到斯芬克斯的比喻。除了古埃及文字以外，基歇尔还研究过希腊语、希伯来语以及叙利亚语。

从某些方面来看，基歇尔和鲁道夫二世十分相似。基歇尔也是一名收藏家。在罗马大学中，基歇尔有一座博物馆，这座博物馆是世界上最早的公共博物馆之一，藏品包括“从钟乳石到鳄鱼标本的各种东西”。[注]此外，基歇尔还拥有一些用途特殊的房间，这些房间里装满了当时最新的科技创新产物。戈德斯通（Goldstone）为我们列出了一些例子，这些科技创新产物包括魔术灯笼（幻灯片投影仪）、温度计、扩音器（基歇尔把各个房间的扩音器连接起来，组成了一套对讲系统）、天体仪、显微镜（基歇尔把显微镜称为“Smicroscopia”）、磁铁、具有欺骗效果的镜子等。在他的天文观测塔的顶端，装有由耶稣会成员操作的望远镜；他还恶作剧般在门厅里的希腊雕像身后装置会发声说话的扩音器，基歇尔还亲切地叫它“德尔斐神谕”。[注]此外，基歇尔还制造了一台磁力钟和一个音乐喷泉。

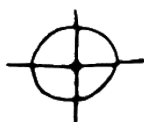
基歇尔与鲁道夫二世的另一个相似之处是：他们都既对科学感兴趣，也对玄学感兴趣。对于艾萨克·牛顿之前的科学家来说，对玄学感兴趣是非常正常的。牛顿被人们称为“最后一位魔法师”。在牛顿之后，科学家才渐渐放弃了对玄学的兴趣。基歇尔和牛顿不同，他并不相信炼金术。然而，基歇尔相信占星术，他还在《地下世界》（*Mundus Subterraneus*）一书中对失踪的大陆亚特兰蒂斯用几页的篇幅做了描写。就破译这份神秘手稿而言，这种将科学和伪科学的各种观念混合在一起的知识结构恐怕并不能算是一种劣势。因为，如果这份手稿中隐藏着与现代科学相左的内容，那么一个像基歇尔这样一只脚在科学世界、另一只脚在玄学世界的人也许反而能够更轻松地理解这份手稿。

遗憾的是，基歇尔没能成功破译这份手稿，准确地说，也有可能他破译了这份手稿，但他没有留下任何痕迹。我们除了知道这份手稿确实曾被寄给基歇尔之外，在基歇尔和这份手稿之间就再没有任何其他已知的联系了。基歇尔从来没有在任何书面文件中提到这份手稿，基歇尔博物馆的目录中详细列明了基歇尔的各种收藏品，然而在这份目录中也找不到这份手稿的身影。你也许怀疑这份手稿在寄给基歇尔的过程中被遗

失了，但是这份手稿后来的历史否认了这种猜测。不管基歇尔的身上有多少过人的能力和素质，但我们几乎可以肯定他并没有揭开这份手稿的秘密。基歇尔的写作数量极为惊人，如果他确实曾成功破译这份手稿的话，我们有理由相信他肯定会在某些作品中提到这次破译的成果。然而，现存的所有文件中都找不到这些信息。

事实上，基歇尔曾以更为公开的方式做出过一些破译密码方面的努力，他曾发表过数篇关于埃及象形文字的著作。人们曾经相信基歇尔已经找到了埃及象形文字的正确解答，他也因此而成了名人。然而，之后的一些工作显示，基歇尔关于埃及象形文字的所谓“解答”事实上是完全错误的。在基歇尔逝世140多年以后，埃及象形文字之谜最终被一个名叫让–弗朗索瓦·商博良（Jean-François Champollion，1790—1832）的法国人成功解开。那么，我们还需要等待多久，才能等到这份神秘的加密手稿最终被正确解答呢？

手稿重现



在基歇尔死后，是否有人继续研究这份神秘的加密手稿？或者在18世纪或19世纪中，有没有人研究过这份手稿呢？这些问题的答案我们都不清楚。鲁道夫二世未能解开这份神秘手稿的秘密，在前文中我们提到的那些智慧博学的人也都未能获得成功。在沉寂了数百年之后，这份手稿再次出现，给20世纪的解密专家们提出了新的挑战。

1912年，一名专营珍稀图书的商人威尔弗里德·伏尼契再次发现了这份手稿。因此，这份手稿现在常常被称为“伏尼契手稿”。1921年时，伏尼契曾在费城做过一次关于这份手稿的讲座，在那次讲座中，他解释

了自己发现这份手稿的经过：

> 为了搜寻各种珍稀的古书和手稿，我会定期游历欧洲大陆。1921年，我正在欧洲大陆访问。在这次访问中，我在一处南欧古堡中意外发现了一批装饰古老华丽的珍贵手稿，它们似乎已经在箱子里尘封许多年了。从当时的情况来看，这些手稿可能从19世纪早期就已经被储藏在那里，躲避了当时欧洲混乱的政治局面。许多手稿上装饰有帕尔马公爵、费拉拉公爵、摩德纳公爵等名门的纹章图案，因此，这些手稿中的大部分应该曾是某些意大利统治家族的私人图书馆的藏品。而现在这些家族已经不复存在了。注

接着，伏尼契对这份加密手稿进行了描述：

> 其他手稿都配有各种金色和彩色的华丽装饰，相比而言这份手稿显得非常丑陋，就像天鹅群中的一只丑小鸭。然而，这种丑陋却立刻激起了我的兴趣。注

根据他对古代手稿的丰富经验，伏尼契估计这份手稿完成于“13世纪后期”。注有了这个成稿日期，再加上这份手稿中涉及的内容非常广泛，伏尼契判断出这份手稿的作者可能是大阿尔伯图斯（Albertus Magnus）或者罗杰·培根。在这两个人中，大阿尔伯图斯没有必要使用密码，而培根曾受过异端法庭的审判，因此他可能有必要对自己的手稿进行加密处理。所以，伏尼契判断，罗杰·培根最有可能是这份手稿的作者。关于这份手稿如何从罗杰·培根手中辗转至鲁道夫二世手中，再从鲁道夫二世手中至基歇尔手中，伏尼契提出了他自己的理论，这套理论我们在前文中已经详细介绍过了。但我们还没有讲到基歇尔死后这份手稿的去向，关于这一点，伏尼契在这次讲座中也进行了解释：

> 帕尔马宫廷中有一些基歇尔的赞助人和朋友，我认为：基歇尔

把这份手稿留给了帕尔马宫廷中的某个人。此后，这份手稿很可能被法尔内塞家族的某位成员拥有，然后和其他手稿一起被带离了帕尔马宫廷，收藏于某座古堡中，也就是我发现这份手稿的那座古堡中。[注]

在这次讲座的最后，伏尼契再次重申了他对这份手稿的来历的猜想：

……我们可以猜测，这份手稿由基歇尔交给了他的一位赞助人，这位赞助人是意大利某统治家族的成员。此后这份手稿一直不见天日，直到1912年被我再次发现。[注]

这篇文章之前曾有一条脚注，解释了伏尼契为什么不愿意透露他购买这份手稿的具体地点。

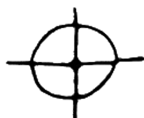
因为我希望能在未来的某天购买这部手稿的其余部分，所以，在此我不准备透露这座城堡的具体位置。[注]

上述这些细节都非常重要，因为我马上就要向读者证明，伏尼契在说谎。

当伏尼契1912年购买这份手稿的时候，手稿中的一些书叶已经遗失。我们之所以能够肯定这一点，是因为这份手稿的书叶标有明确的页码。手稿原件共有116叶，而如今仅存102叶。前文已经说过，这份手稿的每一“叶”包含前页和后页两个部分。因此，正如卡恩（Kahn）及其他一些研究者所指出的那样，这份手稿现存204页，另有28页遗失。有一些来源称，这份手稿共有262页，这是因为他们把手稿中的每个折页计作不止一页。那么，这些缺失的页面以及该手稿的封面是否在鲁道夫二世购买这份手稿时就已经不见了呢？还是说这些缺失的页面是此后才被

移除的呢？这些缺失的书叶中到底包含了怎样的内容呢？

一位图书商人的故事



一位图书商人的生平能有什么激动人心的故事呢？然而，我们要谈论的这一位——伏尼契——的生平确实有其激动人心之处。他的冒险经历遍及欧洲。他的一位雇主曾说："他告诉我们他能说18种语言，确实如此，每一种都说得一样烂。"㊟只要看一看伏尼契的生平，我们就会对他产生许多有趣的怀疑。接下来，我将向读者介绍一些关于伏尼契生平的细节，请读者自行判断这些细节意味着什么。



威尔弗里德·伏尼契生于立陶宛，原名米哈尔·沃伊尼奇（Michal Wojnicz）。他在莫斯科大学获得了化学学位，并成了一名药剂师。药剂师的职业本可以给伏尼契带来安全舒适的生活，但他却并没有沿着这条路走下去，而是参加了摆脱俄罗斯统治、解放波兰的运动。其间，伏尼契参加了营救两名被判死刑的波兰民族主义者的计划，然而计划失败，伏尼契本人也于1885年入狱。但是，伏尼契并没有被判死刑，甚至根本没有被审判，他只是在华沙城堡的一间牢房中被单独关

押了一年。之后，伏尼契单枪匹马成功越狱，并再次参加了解放波兰的斗争。许多年以后，伏尼契指着自己身上的3处伤疤说道："这是一处剑伤，这也是一处剑伤，而这一处是子弹的弹痕。"(注)后来，他又一次被捕，并被送到了东西伯利亚的一个盐矿中服役，然而他再次逃脱。这次逃脱以后，伏尼契没有在当地逗留，而是前往英格兰，并于1890年到达了英格兰。

图1-16 威尔弗里德•伏尼契 (1865—1930)

后来，一位女士描述了这趟英格兰之行的一些细节：

> 伏尼契于1890年逃离了西伯利亚，并到达了德国汉堡。但是他在汉堡却没有任何谋生的手段。当时，德国政府和沙皇政府之间有引渡罪犯的协议，因此伏尼契在汉堡只能藏身于码头、马厩等地。伏尼契靠四处寻得的零星食物充饥，直到他遇上了一艘装满水果、准备前往伦敦的小船。此时，伏尼契已经卖光了他身上所有的东西，包括他的马甲和眼镜。他用身上仅有的钱买了一张三等舱的船票、一条鲱鱼和一些面包。
>
> 接下来，伏尼契在船上度过了一段漫长的旅途。途中这艘小船遇上了风暴，被刮到了斯堪的纳维亚半岛的海岸，并丢失了所有货物。经过这番磨难之后， 伏尼契最终在伦敦的一个码头登陆。此时他身无分文，身上长满了虱子，不仅衣不蔽体，而且饥肠辘辘。
>
> 这是1890年10月5日的傍晚。
>
> 伏尼契不会说英语，因此他只能沿着商人（托尔戈夫）街一直向前走。他手中拿着一张写有一个伦敦地址的纸片，一路向人问路——这张纸片上写着的是朋友斯捷普尼亚克（Stepnyak）的地址。（斯捷普尼亚克先于伏尼契逃到英格兰，在伏尼契第二次越狱之前，斯捷普尼亚克曾联系过伏尼契，并向他提供了自己在伦敦的地址。）最终，伏尼契在街上遇到了一位犹太学生，这位犹太学生在外国人聚集的贫民区中的一家烟草工厂里工作，距离码头不远。这名犹太学生主动走向伏尼契，并且问他："你看起来像是从事政治

活动的人，你是从西伯利亚来的吗？”这位犹太学生给伏尼契带了路，领着他来到了斯捷普尼亚克家中。当晚，斯捷普尼亚克正在家中等待另一位流亡者，以及他的妻子和他妻子的姐妹，还有我和（可能是）费利克斯·沃尔科夫斯基（Felix Volkovsky）。所以，当这位我们不认识的人从码头来到斯捷普尼亚克家里时，我们正好都在。

“这儿又来了一位。”斯捷普尼亚克说道，并向我们解释此人并不是他正在等待的人。

当晚的晚些时候，伏尼契将自己洗漱干净，换上了一套别人的衣服，这套衣服虽然干净，但是穿在他身上并不合体。然后伏尼契转向我，用俄语问道：“我以前是不是见过你？1887年的复活节那天你是否在华沙？”我回答说：“是的，当时我正在去彼得堡的路上。”他又问：“当天你曾站在广场上望着城堡吗？”

我再次回答：“是的。”伏尼契告诉我，当时他正好是那座城堡中的囚徒，那天他从他的牢房中看到了我。此后不久，他就被流放到西伯利亚。注

讲述这段故事的女子名叫埃塞尔·布尔（Ethel Boole），她是著名英国逻辑学家乔治·布尔（George Boole）的女儿。埃塞尔和伏尼契一样是波兰解放运动的积极分子。在伏尼契到达英格兰后不久，他开始与埃塞尔·布尔共同从事革命活动，比如将一些被禁的书籍走私到俄国（这其中包括马克思和恩格斯的著作）。在伦敦，伏尼契以伊万·克莱采夫斯基（Ivan Klecevski）的化名继续从事反对沙皇政府的活动。他之所以使用假名从事这些活动，是因为害怕政府发现他和欧洲某些亲属的关系，那样可能会让这些亲属受到牵连。埃塞尔·布尔使用的化名是布洛奇卡（Bulochka）。1897年，埃塞尔·布尔使用埃塞尔·伏尼契的名字发表了小说《牛虻》，这本小说在俄国流传甚广，此后又在中国流行。《牛虻》一书总共售出了几百万本。当然，埃塞尔·布尔没能收到上述两个国家的图书版税。虽然埃塞尔·布尔早将自己的名字改成了埃塞尔·伏尼

契，但是埃塞尔·布尔和伏尼契两人直到1902年才正式结为夫妇。

此时，伏尼契已经在英国成了一位颇有名望的古董书商。他通过某些途径找到了许多珍稀的书籍，并向外销售。这其中有一些是早已丢失的书籍，还有一些是由伏尼契首次发现的，此前人们根本不知道它们的存在。E.米莉森特·索尔比（E.Millicent Sowerby）是伏尼契书店的一名雇员，她受雇时，我们涉及的这份神秘手稿刚被伏尼契收购不久。索尔比曾经描写过在伏尼契的书店中经常有间谍出没，这些间谍通过各种各样的方式监视伏尼契。

我们有理由相信，这些间谍对古董书交易并没有太大的兴趣。然而，其他书商却对伏尼契获得这些珍稀古书的方式非常感兴趣。伏尼契曾想说服某人加入他的古董书交易活动，他向此人描述了他如何获得这些珍稀的古书：

> 这个世界上有上百万本图书，伟大的珍品不计其数。我在意大利的发现简直令人叹为观止！下面听我说说这件事吧。我曾经到一所修道院中，那里的僧侣向我展示了他们的图书馆。那座图书馆简直是一座金矿，里面充满了古老的印刷书、抄本，以及装饰古老而华美的手稿。当我看到那些珍品的时候，我差点儿昏倒了——我可以向你保证，我几乎当场昏倒在那里。但是我还是让自己保持头脑清醒。我告诉那些僧侣，这些古书不过是一些积满了灰尘的垃圾，我愿意用一套最有趣，并且价值很高的现代神学书籍来交换这些古书。靠着这套说辞，我成功地说服了主管神父。不到一个月，修道院的整个图书馆都归我所有了。而我给他们送去了一车现代垃圾作为交换。现在，接受我的建议吧：辞掉你现在的工作，来做一名图书商人吧。[注]

虽然这次古书收购严格来说不能算是偷窃，但是根据伦敦一所法庭的判决，伏尼契的藏书中确实有一本是从林肯大教堂偷来的。在这场官司的前几年，伏尼契曾说自己“既是一名天主教徒，又是一名不可知论

者”。 ㊟作为不可知论者的伏尼契是否认为宗教机构是理所当然的掠夺对象呢？作为天主教徒的他对此又怎么想呢？

塔拉图塔（Taratuta）写道：

> 他积极参与革命运动。他是波兰社会革命党的成员，属于“无产阶级”的一员。他投身宣传工作，传播非法文献。他拥有一台打字机和一本假护照，他为了革命工作而聚敛钱财。㊟

从上面这段话中我们可以看出，伏尼契有过伪造文件的经历。

根据索尔比的说法，由于第一次世界大战的爆发，伏尼契于1914年离开英格兰前往美国。伏尼契确实在美国纽约开了一家书店，但他也常常去欧洲以战时低廉的价格收购书籍。

第一次世界大战结束以后，伏尼契花费了不少努力，试图破译手头的这份手稿。1919年，伏尼契影印了这份手稿的部分书叶，把这些影印页送给任何他觉得有可能帮助破解的人。伏尼契联系过的专家包括A.G.利特尔（A.G.Little）教授（一位研究罗杰·培根的学者），H.奥莫特（H.Omort，巴黎国家图书馆的一位古文字学家），加斯奎特主教（Cardinal Gasquet，梵蒂冈档案馆主管），美国军方密码专家，以及威廉·纽博尔德教授（Wiuiam Newbold，一会儿我们就要详细讲到这位纽博尔德教授了！）。为了破译这份手稿，伏尼契联系过的专家总共大约有20位。

1921年，伏尼契开价160 000美元出售这份手稿。就算这份手稿的作者真的是罗杰·培根，如果这份手稿根本没人能读懂，伏尼契为什么要开这么高的价呢？伏尼契认为这个开价是公平的，因为宾夕法尼亚大学的纽博尔德教授已经破译了这份手稿的一部分。

威廉·罗曼·纽博尔德是宾夕法尼亚大学智慧与道德哲学系的亚当·塞贝特荣誉教授（Adam Seybert Professor）。纽博尔德教授于1919年首次

宣布，他已经在破译伏尼契手稿的工作中取得了初步成功。他的研究成果显示，罗杰·培根确实是这份手稿的作者。虽然纽博尔德的破译工作非常冗长费时，但是他最终还是破译出了这份手稿中相当数量的文字，足以让他能够举行一个讲座来揭露埋藏了几个世纪的秘密。纽博尔德教授将这篇演讲稿写成了一篇文章，并于1921年4月20日在医师与外科医师学会上做了这次演讲，次日（4月21日）又在美国哲学学会的会议上再次发表了这一演讲。在纽博尔德教授4月20日的讲座之后，伏尼契也做了演讲。伏尼契的演讲内容为听众提供了一些关于这本手稿的背景知识，他解释了这份手稿是如何从罗杰·培根手上辗转到鲁道夫二世手中的。在这两次讲座结束之后，伏尼契和纽博尔德的论文同时发表在《费城医师与外科医师学会学报》（*Transaction of the College of Physicians and Surgeons of Philadelphia*）上，两篇紧挨着彼此。



图1-17 威廉·罗曼·纽博尔德（1865—1926）

约翰·马修斯·曼利（John Mathews Manly）是芝加哥大学英语系教授，也是一位密码专家。曼利参加了纽博尔德的上述讲座。事后，曼利表示，当时“谣言四起”，人们纷纷议论纽博尔德对这份手稿的破译工作究竟会揭示出怎样的秘密。此外，曼利提到，很多与罗杰·培根同时代的人都曾经怀疑罗杰·培根“使用了黑魔法”。曼利还表示：“一些人认为纽博尔德教授掌握了关于黑魔法的秘密。一位可怜的女人不惜奔波数百英里[注]来见纽博尔德，请求纽博尔德使用罗杰·培根的魔法帮她驱走魔鬼。”[注]如果纽博尔德能够在300多年前进行这次演讲，那么鲁道夫二世一定会非常热切地想要聆听这次演讲的内容。

在这次演讲的开始，纽博尔德教授先列举了一些人类历史上的伟大发现，比如首次学会使用工具、发现杠杆、用石头造出锋利刀刃，或冶炼出铜。接着，纽博尔德教授说，人们很少会想到创造这些发现的人，甚至根本就不记得这些发现者的名字。接着，纽博尔德教授描述了显微镜和望远镜这两项仪器的重要性，并且声称，他对手稿的破译结果显示，罗杰·培根知道上述两种仪器的存在，甚至可能是这两种仪器的发明者。然后，纽博尔德教授用大量的篇幅详细描述了罗杰·培根的生平及其贡献，并开始谈他从这份加密手稿中破译出来的内容。纽博尔德教授向读者展示了关于望远镜的证据。他认为，在这份手稿中，其中一幅插图描绘的是仙女座的大星云。由于仙女座的大星云肉眼不可见，所以纽博尔德教授认为，这证明罗杰·培根拥有望远镜。纽博尔德教授这样说：

> 在伏尼契手稿中，罗杰·培根绘制了一幅描绘旋涡星云的插图。如果我的破译结果正确的话，这幅插图旁的一段附加文字写的是：这幅插图描绘的对象是通过“一台凹镜观测到的”，所谓“凹镜”指的就是反射望远镜。我认为，这样的事实确认了我此前提到的结论。这段附加文字解读起来十分困难，因此在经过其他学者确认和修正以前，我不准备将此作为罗杰·培根拥有望远镜的独立证据。[注]

从上面这段话中我们可以看出，学者们在描述自己的结论时非常谨慎。接着，纽博尔德教授继续说道：

> 即使没有伏尼契手稿带来的新证据，在我看来罗杰·培根拥有望远镜也是一个已经确认的事实。但是罗杰·培根是否拥有复式显微镜？或者他拥有的单式显微镜放大能力是否足够帮助他做出真正重要的科学发现？关于这些问题，我们此前没有任何证据。我们最多只能说，由于罗杰·培根拥有一些镜片，并且知道怎样将这些镜

> 片组合起来发挥放大视角的作用，所以罗杰·培根有可能通过组合这些镜片成功地造出了第一台复式显微镜。[注]
>
> 然而现在，关于上述这些疑问已经在很大程度上被伏尼契先生的发现所消除。接下来，我将荣幸地向你们展示这份手稿中的部分插图。插图显示，这份手稿的作者不仅拥有望远镜和显微镜，并且，他所拥有的望远镜和显微镜都具有相当强大的功能。而我已经确认了这份手稿的作者的确为罗杰·培根。证明上述结论的证据是：手稿的最后一页上有一段密钥，这段密钥也被加密了，当我把该密钥代入密码中时，我得到了“R Baconi”这个名字。[注]

接下来，纽博尔德进一步描述了罗杰·培根通过自己的显微镜看到的精子和细胞。纽博尔德认为，这份手稿中的“插图非常清晰地显示了”上述精子和细胞的结构。[注]

> 即便我们无法读懂书稿中的文字，仅仅是插图本身就已经清楚地展示了罗杰·培根的成就。此前，已经有少数学者从已知的证据中得出了以下结论：罗杰·培根拥有望远镜和显微镜，并且很可能是这两种仪器的发明者。然而，大多数学者并不接受上述结论。这份手稿的插图证明，罗杰·培根看到了一些此前人类的眼睛从未看过的解剖结构和天体；事实上，在罗杰·培根身后的若干个世纪中，也没有其他人再次看过这些物体。此外，这份手稿中的插图还显示，罗杰·培根先是构想了一个系统，然后试图用这个先入为主的系统来解释他看到的物体，把他看到的这些物体嵌入这个系统中——他的这种思路主要来自于柏拉图式思维的传统。现在，我们终于能够证明，罗杰·培根是现代科学的真正先驱者，也是富有智慧的不列颠民族所孕育的众多最伟大的天才之一。[注]

接下来，纽博尔德通过幻灯片的形式向听众展示了伏尼契手稿中的一些书叶，并且对手稿中的内容进行了解释。以下是一些重点摘要：

幻灯片29

该图的上角描绘的是卵巢（有核的卵）。（输卵）管打开，我们可以看到一排卵子正向下移至空穴（子宫）中。子宫中共有7个灵魂（精子），其中3个尚没有意识，另外4个表现出了对环境的震惊和恐惧。在下方，8个精子已经找到了他们的“窝”，即8个卵子，它们对自己即将居住的环境表现出惊讶和好奇，然而在这种惊讶和好奇中也混杂着一些厌恶之情。(注)

幻灯片50

这个圆盘状物体和其他几个圆盘状物体一样，与放大的受精卵十分类似。但是，从细节上来看，两者的相似度还不够，因此我们无法把这些图与现代显微镜下看到的受精卵的各种具体发育阶段联系起来。(注)

纽博尔德对手稿中绘制的那些站在桶中的裸体女人有什么看法呢？也许有的读者会对这个问题感到好奇。纽博尔德认为，这些裸女代表的是已经脱离了世俗、踏上回归星辰之路的灵魂。他表示：“这些桶代表的是动物灵魂，而此时精神灵魂还没有完全挣脱动物灵魂的束缚……或者说，这些桶代表的是精神灵魂尚未完全脱离的物质躯体。”(注)

纽博尔德在这次演讲中介绍了上述几个伟大的发现，但是他认为，这份手稿中还有更多的内容等待发掘——因为到发表演讲为止，他只破译了手稿4%的内容。纽博尔德认为，这份手稿中还书写了“秘密中的秘密”，也就是延长人类生命的秘密。如果鲁道夫二世知道这个消息，他一定会非常感兴趣的！

那么，纽博尔德究竟是如何取得以上这些惊人的破译成果的呢？

他的破译方法之一是非常非常仔细地观察手稿中的字母。当他非常

仔细地观察手稿中的字符时，他发现每一个字符事实上是由许多更小的字符构成的。

纽博尔德认为，上述每一个微小的符号都代表一个字母。在此基础上，他分析出了这些符号与字母之间的替代关系，图1–19呈现了这种关系（引自纽博尔德所著的书）。

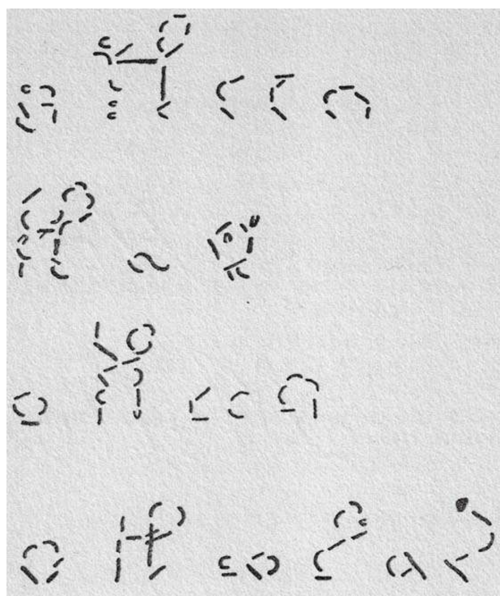


图1-18 字中字的一个样本（根据纽博尔德对这些字的读法）

图1-19 纽博尔德对缩略符号的替换

A
B
C
D
E
H
I
L
M
N
O
P
Q
R
S
T
U V

图1-19 纽博尔德对缩略符号的替换

根据纽博尔德的说法，在完全破译以后，上述这些符号描述的是关于1273年的彗星的信息。但是，这个破译过程绝不轻松。第一，纽博尔德指出，这些微小的字母“只有在显微镜的帮助下才能被看清楚”。[注] 第二，他还说：“这些字母很难辨认，而且其中一些字母非常相似，因此，就目前的阶段来说，在分辨这些字母的过程中产生误差是不可避免的。”[注]除了以上两点困难之外，在破译的过程中还需要解决另一个问题，那就是：即使在使用上述方法取得了这些字母以后，所得到的信息也并不是明文信息。也就是说，在解决了上述两个困难之后，破译的过程才刚刚开始！纽博尔德解释道：“明文信息至少被加密了6层。我可以解开其中的两层。但是要想读到最终的明文信息，还必须进行另外的4项操作。这4项操作中有两项完全是机械式的，然而另外两项（第一项和最后一项）却具有极高的难度，目前我仅仅克服了部分困难。”[注]在纽博尔德所说的这两项困难中，第一项是辨认和读取这些微小的字符，而最后一项是把信息中的字母按照正确的顺序排列起来。纽博尔德透露：“在破译出的最终信息中，我们再次遇到了字母顺序移位的问题。虽然这些字母移位的幅度不大，不会使整个单词变得无法辨认，但是在许多情况下，字母顺序的调换使得我们对培根究竟希望读者读到怎样的信息十分不确定。”[注]上述重新排列的字母（又称“换位”或者“解换位字谜”）可以通过很多不同的方式来完成。纽博尔德认为，培根每次会调换一组字母的顺序，而每一组字母包含55个字母或者110个字母。但是，这种顺序的重排却没有固定的规律。因此，对于每一组字母来说，决定这些字母的正确顺序都可能是一项十分困难的工作。

至此，我已经向读者比较详细地介绍了纽博尔德的破译工作的第一步和最后一步。我不准备详细介绍破译工作的中间步骤，但是我想展示一下纽博尔德完成这些中间步骤的关键工具，即这份手稿的密钥。纽博尔德教授声称该密钥是在手稿的最后一页发现的。图1–20展示了该页手稿中与密钥相关的几行字符。

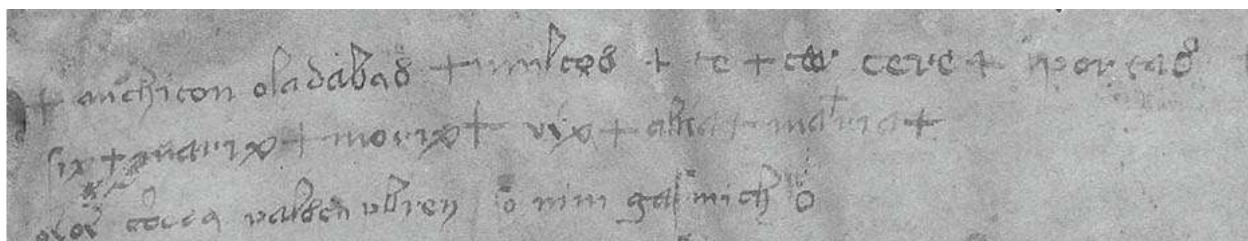


图1-20 “密钥”（手稿第116v叶）

纽博尔德认为，这段文字的开头应该读作：“michiton oladabas multos te tccr cerc portas”。其中，他认为“ton ola te tccr cerc”这部分是“加密元素”，因此除去这部分，这段文字就变成了“michi dabas multos portas”。接着纽博尔德教授把“multos”改为“multas”，他认为这是原文的笔误，这样就得到了一个有意义的拉丁文句子。这句话的意思翻译过来是：“汝赐予我（或者将赐予我）许多扇门。”[注]

接着，纽博尔德教授把这个拉丁文句子中的字母与一组特殊的字母表（该字母表一共包含22个字母，不含J、K、W、X这4个字母）一一对应起来：

MICHIDABASMULTASPORTAS

ABCDEFGHILMNOPQRSTUVYZ

假设纽博尔德提出的这种对应关系确实是一种MASC密码，我们可以用以下两种方法来解读这种密码：

1. 上一行句子是明文，而下方按顺序排列的字母则是明文所对应的密文。也就是M被加密为A，I被加密为B，以此类推。

2. 下方一行字母是明文，而上方的句子则是明文所对应的密文。也就是A被加密为M，B被加密为I，以此类推。

纽博尔德既使用了第一种替换法，又使用了第二种替换法。他把第一种替换法称为主要转换字母表，把第二种替换法称为主要反向字母表。第二种替换方法是有问题的，因为在若干情形下，不同的字母在加密后会变成同一个字母。比如，L、R、Z都被加密成了S。那么当我们进行破译的时候，破译者如何知道字母S究竟代表明文的哪个字母呢？我们到底应该把字母S代换成L、R，还是Z呢？我们将在后文中继续讨论这个问题。

接下来，纽博尔德使用上述字母表，以及含有密钥的这个书叶上的其他难以辨认的笔迹继续制造出了4种“双字母表”和另外8种“辅助双字母表”。为什么要进行上述操作呢？除了纽博尔德自己以外，几乎所有人都不清楚。但是，他所说的“双字母表”的定义是非常清楚的。所谓“双字母表”就是把字母两两组合形成的字母表。今天的密码学家将这种字母组合称为“双字母”（digraph）。纽博尔德的灵感来源是手稿中的一句话——“汝赐予我许多扇门”。在卡巴拉（犹太教神秘哲学的一部分）传统中，“门”这个概念可以指成对的字母。对于我们的字母表而言，双字母的形式如下：

AA AB AC AD … AX AY AZ

BA BB BC BD … BX BY BZ

:: ::

ZA ZB ZC ZD … ZX ZY ZZ

上图中的点代表省略的各对字母，这些被省去的字母与我们写出的字母符合同样的规律。

在纽博尔德完成上述这一系列操作以后，每个字母都与22个字母组成了双字母。

然而这还没有结束，在接下来的步骤中，纽博尔德认为，加密者通

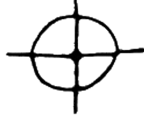
过把发音相似的字母看成是同样的字母而把这份包含22个字母的字母表缩短成包含11个字母的字母表，比如B、F、P都写作P。因此，新的字母表中只有A、P、C、T、E、I、R、M、N、U、S这几个字母。而要想把这个步骤逆转过来（也就是把加密的文字破译出来），破译者就必须加入主观的推测。在密文中的字母P究竟应该被看作字母B、F，还是P呢？答案是这三种情况都可能成立，具体选哪个字母取决于此处的信息究竟是什么。

纽博尔德的方法还有一些其他步骤，但是从上面介绍的这些步骤中我们已经看出，其中有好几个步骤都要求破译者做出自己的主观选择。破译者需要首先辨认出缩写的字符，然后把一份包含11个字母的字母表转化成一份包含22个字母的字母表，最后，破译者还需要重新排列字母的顺序。如果破译者掌握如此大的灵活度，我们就必然会面临这样的风险：破译者可能会做出错误的选择。在这种错误的选择之下，虽然破译者可以破译出一段有意义的文字，但这段文字可能根本不是加密者本来想要表达的信息。

纽博尔德对破译工作进行了如下总结：

> 因此，在取得下一步进展之前，我们对已经破译出来的文字并不应该抱有充分的信心，除了少数情况以外。在这些例外的情况下，破译出的文字给出的是读者事先不知道，但事后已被确认的事实。然而，即使在这些少数的例外情形下，我们也只能确认大概的意思，而不能确认精确的字句。(注)

批评的声音



伏尼契认为纽博尔德的工作应该获得诺贝尔奖——伏尼契当然希望纽博尔德的工作能得奖啦。如果纽博尔德的破译工作真能获得认同，那么科学史将被改写，罗杰·培根可能会成为人类历史上最伟大的科学家，同时，伏尼契的这份手稿也会变成无价之宝。一开始，纽博尔德教授的破译工作确实受到了一些专家的正面评价。

《科学美国人》（*Scientific American*）杂志从1921年5月7日开始报道纽博尔德的工作。一开始，该杂志仅仅刊登了一段很短的消息，内容也相对中立，仅仅宣布该杂志随后将以更大的篇幅报道。1921年6月，这份报道终于出炉，在这篇报道中，该杂志称培根正是这份手稿的作者，但是“对纽博尔德教授的翻译成果却不是特别赞同”。[注]《科学美国人》杂志的主要担忧是，在纽博尔德的工作中，各种替换和换位重排赋予了破译者过高的自由度。

《科学美国人》杂志上还曾发表过另一则报道，日期是1921年5月28日。这篇较短的报道内容大体是对该杂志6月份发表的文章的总结，并且还谈及了手稿中的插图，以及纽博尔德教授对这些插图的解读。这则报道的作者认为：“似乎在某些情况下，纽博尔德教授将个人的意愿凌驾于理性判断之上。”[注]此外，这篇报道的作者还认为，纽博尔德对这份手稿的翻译“完全不合理”。[注]同年6月25日，该杂志又发表了一封信，来自历史学家林恩·索恩戴克。在这封信中，索恩戴克几乎完全认同5月份的报道，唯一的不同之处是他还对培根是不是伏尼契手稿的作者提出了质疑。

约翰·M.曼利在1921年7月的《哈珀杂志》（*Harper’s Magazine*）上也撰文讨论了纽博尔德的工作。曼利似乎两边都不得罪，他既提出了支持纽博尔德的破译结果的证据，也提出了反对纽博尔德的破译结果的证据。也许曼利自己也在感情上举棋不定——曼利从战争年代开始就是纽博尔德的朋友，因此他或许并不想对老朋友提出过于尖锐的批评意见。

但是，曼利本人是英国军情八处的密码专家，因此他显然拥有密码破译领域的许多专业知识。

纽博尔德于1926年9月去世。在他去世以后的几年间，各界对他的工作发出了更激烈的声音。1928年，一本署名为纽博尔德的书出版了。这本书详尽地解释了纽博尔德破译这份手稿时使用的技巧。虽然它展示了许多惊人的破译成果，但很多地方仍然比较模糊。这本书并不像其他书一样是作者本人生前完成，只是死后才发表的。事实上这本书是在纽博尔德死后由他的朋友——同为宾夕法尼亚大学教授的罗兰·格拉布·肯特（Roland Grubb Kent）根据纽博尔德的笔记汇总完成的。

1929年，林恩·索恩戴克再次发声，发表了书评。这次，索恩戴克已经不仅仅是质疑罗杰·培根是不是这本书的作者了。他在书评中这样写道："罗杰·培根与伏尼契手稿能扯上关系的概率还不到五十分之一。"注

此时，纽博尔德的朋友曼利也不再像此前那样举棋不定了，他也转而反对纽博尔德教授。在1931年的《宝鉴》（*Speculum*）杂志上，曼利发表了一篇文章，其中出现了以下这段措辞坚决的言论："我的意见是，纽博尔德的成果是完全没有根据的，因此我们绝对应该彻底否定他的结论。"注曼利对自己此前一直保持沉默的原因做出了如下的解释：

> 法国最杰出的哲学家之一——吉尔松（Gilson）教授虽然对破译的方法感到迷惑，但是却接受了破译的结果；研究罗杰·培根的著名专家拉乌尔·卡顿（Raoul Carton）教授发表了两篇很长的论文，热情地肯定了破译的方法和结果；美国的化学家和生物学家也同样给予了正面的评价。出于对科学真理的追求，我们应该仔细地研究纽博尔德对这份手稿的破译结果。注

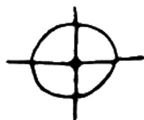
在所有这些声音中，并没有人怀疑纽博尔德作假或者故意欺瞒，所有人都相信他的正直和诚实。曼利认为，他的破译成果是"纽博尔德教

授自身的热情和智慧通过他的潜意识创作的一件作品”。(注)

在我看来，纽博尔德教授从手稿中辨认出的这些“缩略符号”的碎片都只不过是手稿笔迹中的墨水由于长时间的作用而变得斑驳而已。手稿使用的皮纸极不光滑，使用的墨水也不是染色剂，而是一种相当浓稠的颜料。这种颜料在风干的过程中，产生了不均匀的沉淀以及一些裂痕，纽博尔德教授却把这些痕迹视为需要用显微镜检视的密码。以下这些古文字学家都同意我的上述观点，他们包括芝加哥的比森（Beeson）教授和厄尔曼（Ullman）教授，维也纳的弗里茨（Fritz）教授，伦敦的罗伯特·斯蒂尔（Robert Steele）先生，以及大英博物馆的弗雷德里克·凯尼恩（Frederic Kenyon）爵士以及埃里克·米勒（Eric Millar）先生。(注)

曼利在该文中还写道：“我们只能寄希望于一位与纽博尔德教授同样充满勇气和献身精神的人能够利用比他更合理的方法，再次对伏尼契手稿中的神秘密码展开新的攻势。”(注)

备受冷落的手稿



伏尼契于1930年去世，他并没有听到曼利对纽博尔德破译成果的尖锐批评。根据伏尼契的遗嘱，这份著名的手稿由他的遗孀和秘书安妮·M.尼尔（Anne M.Nill）共同继承。此外，伏尼契还在遗嘱中规定，如果有任何公共机构出价100 000美元以上，那么继承人就可以把这份手稿出售给该公共机构；同时，遗嘱不允许继承人把这份手稿出售给任何

私人机构。然而，有了曼利的这篇论文，谁还愿意出这么高的价购买这份手稿呢？由于找不到合适的买家，伏尼契的遗孀埃塞尔·伏尼契将这份手稿放进了一个保险箱中，直到她1960年去世。

由于伏尼契始终拒绝透露这份手稿究竟于何处购得，所以人们自然会怀疑这份手稿也许根本就是伏尼契自己伪造出来的。毕竟，伏尼契是一名古董书商，他完全有可能找到足够数量的空白皮纸，并在这些皮纸上画出奇怪的文字和插图。事实上，伏尼契在伦敦开的书店的一位雇员宣称，伏尼契曾以每张一先令的价格向一位名叫詹姆斯·麦克贝（James McBey）的画家出售过空白的15世纪的皮纸。同样，能部分证明这份手稿的来源的那些书信也完全可能是伏尼契伪造的。在一篇1986年发表的论文中，迈克尔·巴洛（Michael Barlow）提出了这样的推测：这些书信本身可能是真实的，但是这些书信与这份加密手稿之间却没有任何联系。巴洛认为，这份手稿可能是伏尼契伪造出来的，伏尼契通过把这份伪造的手稿与这些真实的书信联系起来而增加这份手稿的可信度。

然而，如果这份手稿确实是伏尼契伪造出来的话，为什么他要在遗嘱中规定继承人不得将这份手稿出售给个人呢？从遗嘱中的这条规定来看，他似乎希望这份手稿能够被存放在学者们可以企及的地方。也就是说，伏尼契似乎确实把这份手稿看作科学史上一份很有价值的文件。

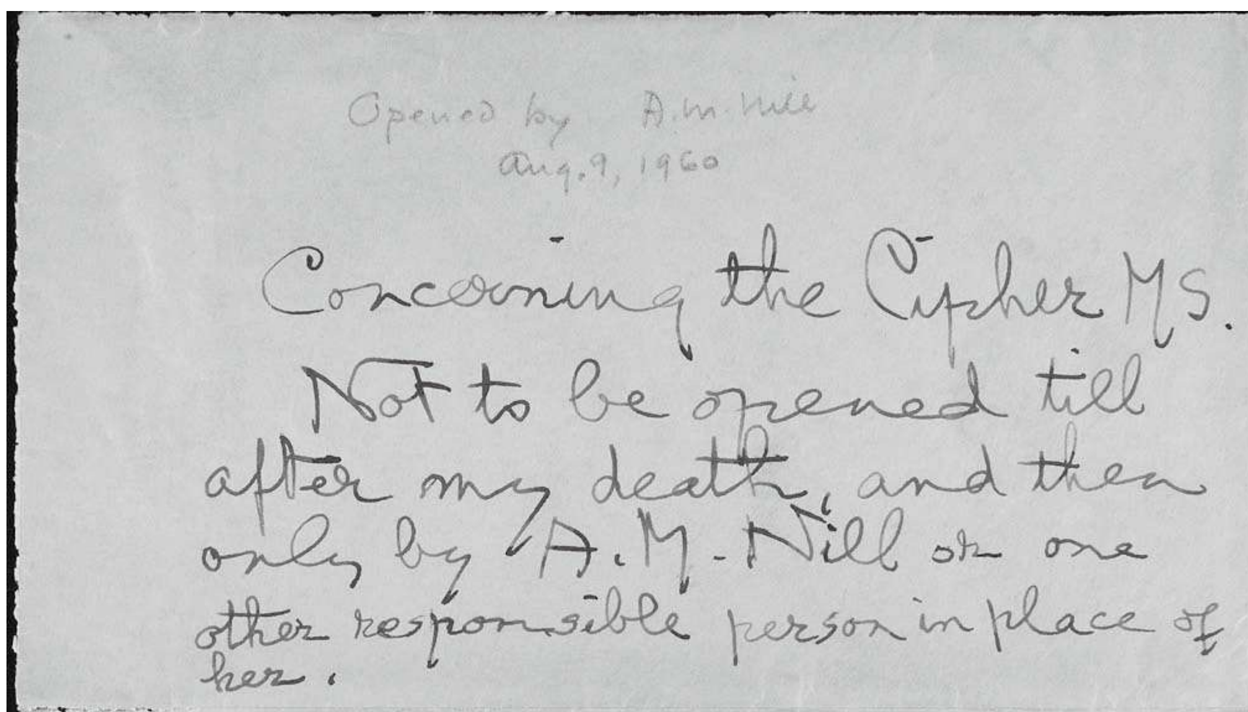


图1-21 装有关于加密手稿信息的信封

埃塞尔·伏尼契去世后，伏尼契的秘书尼尔继承了一个奇怪的信封，它似乎能够帮助我们回答另外一个问题。

埃塞尔·伏尼契留下的这个信封上写着“关于加密手稿”的字样，这个信封上还标有以下提示：“在我死前不得打开。死后只能由A.M.尼尔或者其他人代她打开。”

这份加密手稿究竟有什么秘密是不能在埃塞尔·伏尼契死前揭开的呢？在这个奇怪的信封中，有一封两页长的信，写在了伏尼契的丈夫的信纸上，内容如下：

> 这封加密手稿以及其他手稿是W.M.伏尼契于1911年，或者于1911年左右购入的。这份手稿曾经归梵蒂冈罗马教廷所有，并且曾经藏于弗拉斯卡蒂（的一个城堡中？）。伏尼契通过一位中间人接触梵蒂冈当局，这位中间人是英国耶稣会神父约瑟夫·斯特里克兰（Joseph Strickland）注，我个人相信斯特里克兰曾与马耳他有一些联系。斯特里克兰神父知晓内情，即如果能够找到谨慎可信的

买家，梵蒂冈当局会安排出售某些特定的手稿。我不知道这桩交易需要保密是不是因为当时梵蒂冈与意大利政府的关系紧张[注]。斯特里克兰神父以个人名义担保W.M.V是可以信任的。由于这一保证，在伏尼契做出保密承诺后，他被允许购买这份手稿（原文如此）。斯特里克兰神父当时秘密地告诉我这些情况，是因为他认为万一自己死了的话，应该有人知道这个秘密。这件事过后不久，斯特里克兰神父就去世了。出于和他同样的原因，我在保险箱中留下了这份声明，以便在我死后有人能读到这些内容。

埃塞尔·伏尼契

1930年7月19日

信中提到的地点——弗拉斯卡蒂——指的是蒙德拉戈内别墅，那里曾经是一处耶稣会学院，但资金极度缺乏。它就位于距离罗马不远的弗拉斯卡蒂。

伏尼契在这封信里叙述的故事和他生前的说法很不一样（伏尼契声称这份手稿是他在“帕尔马公爵”、“费拉拉公爵”，以及“摩德纳公爵”的藏品中发现的）。有了这封信里提供的新信息，我们就能把基歇尔和伏尼契联系起来了。基歇尔死后，他多年来收到并保存下来的信件被送到了第一座耶稣会大学的图书馆，即罗马大学的图书馆。这所大学今天仍然存在，现在叫宗座额我略大学。巴雷什和马尔奇写给基歇尔的信正是在宗座额我略大学被发现的。

虽然没有坚实可信的记载，但是这份加密手稿极有可能也被送到了罗马大学的图书馆中。证明这一点的证据来自该手稿后一任主人的身份，我将在下文具体讨论这个问题。1870年，罗马还是个独立的国家，当年，维托里奥·埃马努埃莱二世在统一意大利的过程中入侵了罗马。在这次侵略中，教会的许多资产被新政府没收，这其中就包括罗马大学图书馆的藏书。但是，由于当时规定大学教职人员的个人藏书不在没收的范围之内，所以在罗马大学的图书馆被政府没收之前，该图书馆的不

少藏书被转移成为教职人员的个人藏书。皮埃尔·让·贝克（Pierre Jean Beckx，1795—1887）注就是这些教职人员中的一员，当时他是罗马大学的校长以及蒙德拉戈内别墅耶稣会的第22任负责人。在这股为了躲避政府没收而转移藏书的风潮中，贝克的个人藏书得到了极大的丰富。

为了保证藏书的安全，贝克把他的“个人图书馆”搬进了蒙德拉戈内别墅。在得知伏尼契是在蒙德拉戈内别墅购买的这份加密手稿以后，我们自然想到研究他在同一地点购买的另外30份书稿。有趣的是，在这批手稿中，几乎所有手稿的封面上都注明了所有人的名字：彼得鲁斯·贝克（即皮埃尔·让·贝克）。既然所有者名字的标注完好地保存在伏尼契收购的所有其他手稿上，那么，如果这份神秘手稿上也曾有过所有者的名字，伏尼契为什么要抹去这个名字呢？

考虑到伏尼契的这种行为，加上他一直拒绝透露获得这份手稿的具体地点，我们有理由怀疑这份手稿也许是伏尼契偷来的。我在本章前面已经向读者提供了一些伏尼契的生平经历，读者可以自行判断偷窃手稿的行为是否符合伏尼契的个性。



图1-22 安妮·M.尼尔（1894—1961）

先不管伏尼契为什么要隐藏这份手稿的真正来源，在伏尼契及其夫人双双去世以后，如何处理这份手稿的决策就落到了尼尔的手中。此时，她成了这份手稿的唯一所有人，她决定出售这份手稿。

尼尔很快为这份手稿找到了买家。1961年，尼尔以24 500美元的价格把伏尼契手稿卖给了汉斯·P.克劳斯（Hans P.Kraus）。克劳斯是一名犹太人，他曾两度陷入纳粹集中营中（达豪集中营和布痕瓦尔德集中

营）。此后，克劳斯携带一份非常珍贵的文件——哥伦布1494年写的一封书信的副本于哥伦布日到达美国，并在那里成为一名成功的古董书商。

在自传中，克劳斯写道：

> 1963年我在罗马，并在梵蒂冈图书馆拜访了若泽·勒伊斯哈特蒙席(注)。我知道勒伊斯哈特蒙席曾编纂出版过蒙德拉戈内图书馆的目录，因此我希望能从他那里获得关于这份加密手稿的信息。让我极为惊讶的是，他认为这份手稿仍在该图书馆中。(注)

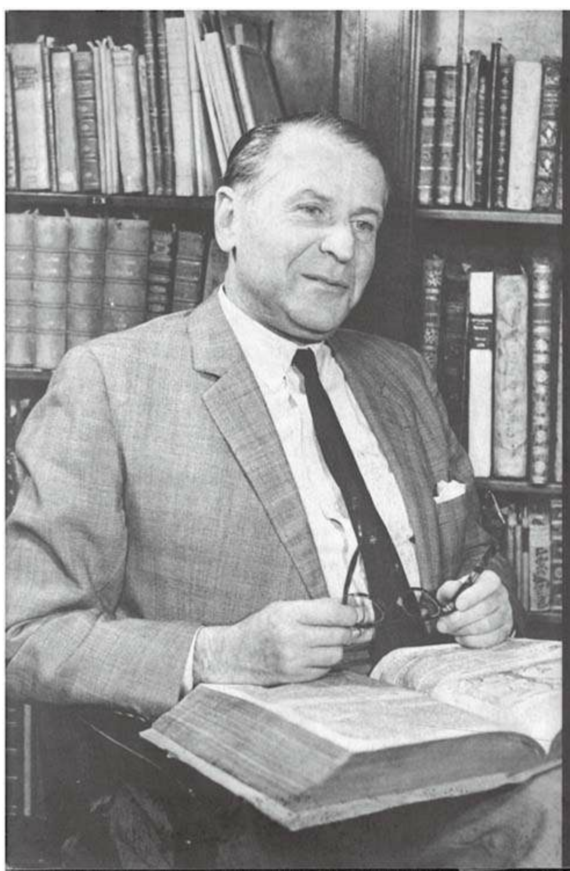
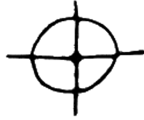


图1-23 汉斯·P.克劳斯(1907—1988)

如果伏尼契合法地购买了这份手稿，为什么勒伊斯哈特会认为这份手稿仍在蒙德拉戈内图书馆中呢？

克劳斯并没有出售这份手稿，而是于1969年把这份手稿交给了耶鲁大学专门收藏珍稀图书及珍稀手稿的拜内克古籍善本图书馆，同时还把一箱关于这份手稿的书信、小册子、笔记以及其他文献也交给了该图书馆。伏尼契手稿至今仍收藏在耶鲁大学的拜内克古籍善本图书馆中，它在该图书馆目录中的编号是408号。

其他“解答”



纽博尔德的破译结果虽然没有获得专家的认同，却赢得了媒体的大量关注。伏尼契手稿的其他研究者提出的破译结果再也没有能够引起像纽博尔德那么大的反响。但在这些年中，仍然涌现出了很多其他的解法。(注)接下来，我将伏尼契手稿的一些其他破译结果简单列举出来。由于篇幅的限制，在此我没有办法与读者一起详细地分析这些破译结果。如果读者希望了解更多这方面的信息，可以参考本书末尾的参考书目。

约瑟夫·马丁·菲利（Joseph Martin Feely），1943

约瑟夫·马丁·菲利是纽约罗切斯特的一名律师，他雇用了一个研究团队来帮他统计这份手稿的字母出现频率，并与罗杰·培根其他著作的字母出现频率相比较。在完成了上述工作以后，菲利得到了以下结论：伏尼契手稿的作者确实是培根，这份手稿先以缩写的拉丁文写成，再使用MASC密码加密。菲利破译出来的明文是一份主要讲述妇科学的科学文献。此前，菲利还曾经发表过关于莎士比亚作品中隐藏的密码的论文。在《未解之谜（下）》的第7章中，我们还会看到他在破解另一份密码方面的成绩。

莱昂内尔·克拉伦斯·斯特朗博士（Dr. Leonell Clarence Strong），1945

莱昂内尔·克拉伦斯·斯特朗博士是耶鲁大学的一位遗传学家和癌症研究者，他将自己关于这份加密手稿的想法发表在了顶级学术期刊《科学》上。(注)和传统的观点不同，斯特朗认为这份手稿的作者是安东尼·阿斯卡姆（Anthony　Askham）。根据斯特朗的说法，这份手稿“使用了

一种特殊的双重等差数列系统对多重字母编码”。斯特朗没有进一步解释这句话的含义，而是写道：“然而，由于目前的战争局势，现在似乎并不是非常适合发表密钥的细节。”斯特朗破译出来的内容是用中世纪英语写成的，这部分手稿主要涉及的内容是：“第一，植物对于健康和疾病的生理过程的影响，尤其是对女性疾病的影响；第二，哈维时代以前的生育和分娩观念。”手稿中“数次提到了抗生素的使用”。某份报纸以通俗的语言对破译出的这部分内容做了以下描述：“（手稿）对妇科疾病以及夫妻间的一些实际问题进行了非常坦率的讨论。”[注]

罗伯特·S.布伦博博士，1974—1975

与纽博尔德一样，罗伯特·S.布伦博博士也是一名哲学教授，但他之前还是美国军方的情报工作人员。此外，和这本手稿的其他研究者相比，布伦博还有另外的一个优势，那就是他在耶鲁大学工作。自从克劳斯将伏尼契手稿捐给耶鲁大学图书馆以后，这份手稿就一直保存在耶鲁大学。[注]

布伦博先是在《宝鉴》杂志上发表了一篇简短的文章。在这篇文章中，他宣布自己在破译伏尼契手稿的工作中取得了突破性的成果，并承诺很快会将破译工作详细发表在《耶鲁图书馆学报》（*Yale Library Gazette*）杂志上。这篇文章的结尾处，布伦博博士对纽博尔德视作密钥的那条文字提出了一种新的解读。布伦博对这句密钥的读法和纽博尔德教授不同，他认为这句密钥应该是“MICHI CON OLADABA ”。接着布伦博将“OLADABA”一词中的每一个字母前移3位（尤利乌斯·恺撒就是这么加密的），于是就得到了“RODGD”一词。布伦博认为“RODGD”一词应该被读作“ROGER”。接着，他又从密钥中取出另外两个词CON和BA，并且通过字母重排得到“BACON”一词。因此，最后的完整结果就是“MICHI ROGER BACON”，意为“我罗杰·培根”。布伦博认为此前的一些研究已经证明，培根并不是真正的执笔

人。但他认为这份手稿中的密钥以及其他部分文字也有可能誊抄自一个年代更加古老的来源。还有一种可能性是，某个人（比如约翰·迪伊或者爱德华·凯利）伪造了这条包含手稿作者署名的密码，以误导潜在的买家，让他们相信罗杰·培根就是这份手稿的作者。

在前文中，我已经展示了这条密钥的图片（图1–20）。从那张图片上，我们一共可以看到3行文字。布伦博认为，第3行文字去掉开头的两个字，就可以得到“valsch ubren so nim ga nicht o”。这个句子看上去像是残缺不全、拼写错误的德语，意思为：“以上是虚假的，所以不要相信它。”因此布伦博认为，这条证据进一步说明，不应该太认真地对待这条所谓的密钥。

在发表于《耶鲁图书馆学报》上的论文中，布伦博提出，这份手稿是根据以下的字母替换规则加密的：

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z (-US)

1 2 3 4 5 6 7 8 9 1 2 3 4 5 6 7 8 2 4 6 8 1 3 5 7 9 (9)

虽然上面的这份替换字母表看起来非常简单，但是破译者面临的不确定性仍然很高。布伦博给出了以下的这个字母表格，并指出使用这份字母表格就能将密文译为明文：

1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I
J	K	L	M	N	O	P	Q	
	R		S		T		U	-US
V		W	(X)	X		Y		Z(?)

比如，让我们来考虑这样一段密文：“２８２４６４５２１３６５６５９６”。要想破译这段密文，我们就必须在每个数字下面写出这个数字可能代表的所有字母：

2	8	2	4	6	4	5	2	1	3	6	5	6	5	9	6
B	H	B	D	F	D	E	B	A	C	F	E	F	E	I	F
K	Q	K	M	O	M	N	K	J	L	O	N	O	N	-US	O
R	U	R	S	T	S	X	R	V	W	T	X	T	X	Z	T
			X		X										

接下来，我们需要在每一个竖列中选出一个字母，以保证这些字母连在一起能够形成一段有意义的信息。但是，这条信息到底是以“BURST”开头，还是以“RUB”开头呢？感兴趣的读者可以自行尝试，看看你们能否判断出明文信息究竟是什么。

除了上述这重困难以外，用来加密这份手稿的9个数字还被加上了另一重伪装，那就是加密者会以不同的方式书写这9个数字。因此，我们得到的伏尼契字母表比上述字母表规模更大。

就算解决了以上的所有问题，我们仍然无法得到一眼就能看懂的明文信息，因为伏尼契手稿是用一种“人造语言”写成的。“这种人造语言

以拉丁语为基础，但并非严格地以拉丁语为基础。它的拼写方式在语音上很不成体系。手稿中的某些段落看起来完全是在用重复的文字来充数。”㊟此外，布伦博还认为，在伏尼契手稿中，每8页密钥就会发生轻微的变化。由于布伦博的破译结果并不能读得通，他后来又怀疑伏尼契手稿可能还有更深层次的加密——也许，他破译出来的每个单词事实上只代表一个字母，或者只是手稿中部分有意让人读出来的单词。

J.R.蔡尔德（J.R.Child），1976

J.R.蔡尔德是一位供职于美国国家安全局的语言学家。他在《美国国家安全局技术期刊》（*NSA Technical Journal*）上发表了一篇保密论文，该论文指出：伏尼契手稿“是用一种目前尚不明确的中世纪德国北部方言写成的”。㊟目前蔡尔德的这篇文章已经被解除保密，感兴趣的读者可以查阅该文，并自行判断蔡尔德提出的证据是否合理。2007年，蔡尔德又发表了另一篇论文，提供了进一步的证据。在这篇2007年的论文中，蔡尔德的说法比前一篇论文稍微笼统一些，他写道：“我很有信心地认为，这份手稿是用一种日耳曼语族的语言写成的……”㊟

约翰·斯托伊科（John Stojko），1978

约翰·斯托伊科是乌克兰的一位业余研究者。他认为，伏尼契手稿的明文是用乌克兰文写成的，在进行加密之前，加密者先移除了手稿中的所有元音字母，以增加破译的难度。

利奥·列维托夫博士（Dr. Leo Levitov），1987

中世纪时有一个基督教派叫作卡特里派，这个教派和圣殿骑士团有

一些相似之处，也和圣殿骑士团一样受到天主教会的镇压。利奥·列维托夫博士认为，伏尼契手稿与卡特里派有关。列维托夫是一位生活在美国新泽西州的医生，也是一名“二战”老兵。他认为，伏尼契手稿并非密文，而是“用一种融合了多种语言的中世纪佛兰芒语写成的，其中含有大量从古法语以及古高地德语中借来的词汇”。[注]

吉姆·E.芬恩（Jim E.Finn），2001

吉姆·E.芬恩认为，伏尼契手稿其实是希伯来语。芬恩提出了这样一个问题：这份手稿会不会是由诺斯特拉达穆斯[注]创造的，或者会不会是一本占卜者使用的书呢？芬恩的破译结果可以在一个网站上找到，只要从这个网站上引用几句话，我们就能够大致了解芬恩的破译结果是什么风格了。这个网站上写道：“伏尼契手稿最可能是中世纪时外星人和不明飞行物昭示人类末日的文件的一部分。”此外，该网站上还写道：“他破译出来的几页似乎是在谈论一个‘天眼’在地球引发的周期性大洪水。”人类的末日究竟何时来临？芬恩的破译结果似乎来得很及时，因为他警告我们说：“我们也许能够亲眼见证末日的到来。”[注]

兹比格涅夫·鲍瑙希克（Zbigniew Banasik），2003

这位波兰研究者提出的破译结果可能是把该手稿的年代判断得最早的结果之一。兹比格涅夫·鲍瑙希克写道：“这份手稿可能是在公元前几个世纪写成的。”他认为，这份手稿使用的语言应该是满语的前身。[注]

比阿特丽斯·格温（Beatrice Gwynn），2004或更早

格温是都柏林人。她曾在布莱奇利园的非密码部门工作过。[注]格温

认为，伏尼契手稿是用“镜像中高地德语”注写成的。也就是说，作者书写的文字是镜子中的倒影，只要把手稿放在镜子前面，就可以看到手稿内容的明文（明文为中高地德语）。列奥纳多·达·芬奇就曾使用过镜像文字进行书写，由此可知镜像文字的概念在16世纪以前就已经有了。格温认为，伏尼契手稿完成于16世纪，是一本卫生学手册。

乌尔苏拉·帕普克和迪尔克·魏德曼（Ursula Papke And Dirk Weydemann），2005

2005年，这两位德国人发表了一份新闻通讯稿（当然是用德语写成的），声称他们已经成功破译了伏尼契手稿。这份新闻通讯稿的部分译文如下：

> 这本书以独特而准确的文字和插图，描述了人类可以如何使用遍布整个宇宙的所有能量。在中国，这种能量被称为“气”；在印度，这种能量被称为“昆达里尼”或者“普拉那”；而基督教徒则将这种能量称为“光”或者“圣灵”。这本手稿描述了一种途径，通过它，人类可以在灵魂上获得发展，上升到更高的层次。这一过程从一个人最核心的部分开始，以一种内在提升过程为实现形式，最终会完成生命的循环。这其中，人的心扮演了一种核心的角色。只有爱施展出全部的转化力量，人才能到达最高的层次。注

这份新闻通讯稿还声称，他们将会把整部手稿的破译结果翻译成德语和英语，并发布在以下网址上：www.ms408.com。但是当我试图访问这个网址时，却只看到了“该域名可供出售”的信息。然而，点击以下网址可以看到翻译后的一页手稿，并且还能链接到更多发布手稿翻译的页面，这个网址是：http://www.ms408.de/translation_d.htm。在这些网页中，这份手稿有13叶已经被翻译为德语。目前尚没有该手稿的英语翻译

版本。

在帕普克和魏德曼的破译方法中，他们认为伏尼契手稿中的字符并不是加密的文字，而只是对一些概念的描绘。

> 因此，我们怀疑，408号文件或者“最终原件”曾被秘教社团用作教科书，目的是学习以及传递更高的知觉层次。[注]

此外，另一位德国人乔纳森·迪拉斯（Jonathan Dilas）提出了一种截然不同的破译结果，不过他的破译结果无法用简单的语言总结出来。

伊迪丝·舍伍德博士（Dr. Edith Sherwood），2008

虽然伊迪丝·舍伍德博士没有给出具体的破译结果，但是她提出该手稿的作者是童年的列奥纳多·达·芬奇。舍伍德认为，手稿完成时达·芬奇大约在8~10岁左右。舍伍德认为，手稿“很可能是由变换了字母顺序的意大利语，以带有华丽装饰的花体字写成”。[注]

乔迪·马特（Jody Maat），2009

这位研究者认为，伏尼契手稿是用“古荷兰语”写成的。他把一些破译成果发布在了网络上，以下是他的一些发现：

> 伏尼契手稿的作者是一个名叫德里奇（de Rici）的人。德里奇肩负使命向世界的另一侧航行，去往不被太阳照耀的地方。他用星辰为自己的船导航，最终到达了目的地。德里奇发现这里没有太阳的照耀，甚至还有陆地。于是，德里奇把他看到的景象绘制成图，并且用文字描述了他看到这些景象的地点。同时他也意识到，他的

> 这些发现很可能会使祖国的人民大为震惊，人们可能不会相信他的说法。因此，德里奇以这样的一句话结束了他的这份手稿：“IT IS AS IT IS THAT IS THE TRUTH.（一切就是这样，这就是真相。）”㊟

理查德·罗杰斯（Richard Rogers），2009

理查德·罗杰斯是一名美国陆军/海军计算机程序员，他号称拥有“古代历史、语言学以及计算机科学”的学位。罗杰斯对伏尼契手稿进行了复杂的解释。另一位研究者尼克·佩林（Nick　Pelling，他本人也曾写过一本关于伏尼契手稿的书）对罗杰斯的破译工作进行过如下的描述：

> 我花了很长时间才刚刚开始理解理查德·罗杰斯认为自己在伏尼契手稿中看到的东西，而我至今仍然无法理解他为什么会这么想，也无法理解他是如何从（a）认为这份手稿中存在有意义的内容，跳到（b）看出这些有意义的内容究竟是如何表达出来的。正是由于这个原因，我几次试图发表对于罗杰斯的工作的看法，但每次都在中途放弃了。但是，既然现在罗杰斯已经把他的结果公之于众，我想我也只能尽我所能完成这一工作了……㊟

如果某个人的破译结果甚至没有办法让其他专家理解，那么这种破译结果几乎肯定是错误的。

维科·拉特瓦拉（Viekko Latvala），2011

维科·拉特瓦拉是一位芬兰商人，他声称在某种“更高层次的力量”的帮助下得到了伏尼契手稿的破译结果。拉特瓦拉称自己是“上帝的预言者”，他称伏尼契手稿是包含了一个预言的“声波和音节”。㊟拉特

瓦拉说，手稿中做出的预测“甚至延伸至这本手稿诞生的数十年甚至数百年之后”。[注]拉特瓦拉的一位生意伙伴阿里·凯托拉（Ari Ketola）拒绝解释拉特瓦拉是如何破译这份手稿的。但是凯托拉说：“拉特瓦拉声称任何‘正常人类’都不可能破译这份手稿，因为没有任何密码或方法能够让人类读懂这些文字，这是一种先知使用的传输语言。能读懂它的人很少，然而从千禧年直到今天，这类人却一直存在于世界上——维科·拉特瓦拉先生在过去20年中一直拥有这种神赐的天赋。”[注]

2014年是伏尼契手稿的破译成果大量涌现的一年。接下来我将介绍3种2014年发表的破译结果。

斯蒂芬·巴克斯（Stephen Bax），2014

斯蒂芬·巴克斯是贝德福德大学应用语言系的教授，他破译了伏尼契手稿中的“大约10个单词，以及14种符号和部分”。[注]他认为，这份手稿“很可能是一篇关于自然的论文，并且可能是用近东或者亚洲语言写成的”。[注]关于他的详细破译成果可以参见他个人网站上的一篇长达62页的论文。此外，巴克斯还把自己的破译成果做成了一个视频放在YouTube网站上。

阿瑟·塔克博士（Dr. Arthur Tucker），2014

阿瑟·塔克博士提出了一种全新的理论，他认为伏尼契手稿是用一种已经失传的那瓦特尔语（Nahuatl）写成的。那瓦特尔语是阿兹特克人使用的语言。

韦恩·J.保罗（Wayne J.Paul），2014

从他的个人网站上直接引用的这段文字用来概括他的研究成果是再好不过的了：

> 人类也许永远无法“理解”伏尼契手稿中的符号和文字的确切意思。因为伏尼契手稿是用一种天使语言写成的，它是拿非利人（拿非利人是《圣经》中描写的一种巨人，由上帝的堕落的天使与人类女子结合而生）在学校里教授儿童所使用的教科书。拿非利人曾用一本古代的教科书来教育他们半人类的儿童，而伏尼契手稿是这本古代教科书的一份15世纪的抄本，这本教科书历经大洪水，却奇迹般地留存到15世纪早期。它一定已经残破不堪，因此把它重新誊抄为伏尼契手稿一定花费了手稿作者不少的工夫。但是，这些抄本在当时还是可以被读懂的，否则，手稿的作者就不会花那么多精力和金钱来复制其中的内容。(注)

奥列格·莱恩斯（Олег Лайонс），2015

奥列格·莱恩斯的理论是，一位商人在15世纪的某个时间从意大利北部来到了中国。这位商人在中国停留了很长时间，所以他不仅能流利地说中文，还能够熟练地阅读和书写中文。在回到意大利以后，这位商人发现自己需要一些资金。

于是他找出了一本书（也许这是他拥有的唯一一本书），并将这本书翻译成了中文。然后，他将这本书的中文译本重新罗马化（使用某种拼音方案），并用自己发明的字母重写了这部书（每一个字符都对应于拉丁语字母表上的一个字母）。此外，这位商人还在书中添加了一些无意义的字符和一些拉丁文的批注，并加入了一些复杂的插图。于是，这位商人便创造了一本所谓的“收藏珍品”。(注)

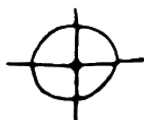
莱恩斯声称，这位意大利商人“收到的钱比他想象中还要多，这不仅解决了他的经济问题，还使他重新走上了经商的道路，并获得了巨大

的成功”。

关于这份手稿的理论和所谓的“破译成果”还有许多，感兴趣的读者可以在以下网址上找到这些内容：http://www.ciphermysteries.com/the-voynich-manuscript/voynich-theories。

从所有这些所谓的“破译结果”中，我们可以得到怎样的结论呢？在这些破译结果中，有些结果来自受教育程度很高的研究者，比如纽博尔德教授，因此这部分结果是值得我们仔细研究的。而另外一些所谓的“破译成果”则完全可以立刻否定。然而，即使是这些非常荒谬的“破译成果”也获得了新闻媒体的头条关注。也许我们从中应该学到的教训是：下次如果再有人宣布他破译了伏尼契手稿，我们可千万不要太过兴奋了。

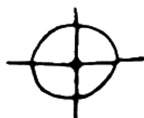
20世纪的研究成果



在19世纪，人类取得了许多重大的破译结果。然而具有讽刺意味的是，这些研究成果破译的并不是密码，只是一些明文语言，比如古埃及人使用的象形文字、古波斯语、阿卡德语、苏美尔语等。我们花了巨大的精力，成功破译了这些当时任何识字的人都能轻易读懂的内容。

我们有理由相信，至少有一位生活年代比上述人群晚得多的人能够读懂我们想要破译的这份伏尼契手稿，即它的作者。那么，为什么20世纪的破译技术竟然都不能成功破解它呢？在20世纪，人类为了破译伏尼契手稿花费了巨大的努力，这其中包括了美国国家安全局及英国相应机构（政府通信总部，GCHQ）顶级专家的努力。

改写的字符



所有想要破译伏尼契手稿的人都必须先做两件事，一是获得一份该手稿的副本（当然！），二是改写手稿中的字符。也就是说，破译者必须把手稿中的字符用字母和数字表示出来，这样才能比较轻松地把这份手稿录入计算机，并与其他研究者分享。而且，完成上述工作以后，研究者就能更容易地统计手稿中的字母频率以及字母组合频率，并且能够利用计算机进行统计检验。任何现代密码学家在破译伏尼契手稿的时候都会用上计算机这一有力的工具！

在20世纪，许多伏尼契手稿的研究者都是用副本的副本作为研究对象的。虽然丁佩里奥（Mary D’Imperio）和弗里德曼（William F.Friedman）都在美国国家安全局工作，但是丁佩里奥的副本与弗里德曼的副本就有四五处差异。副本有时候会出现页面边缘处对焦不准的问题，还有一些页面会部分缺失。许多副本上都有早先的破译者留下的标记。约瑟夫·菲利是号称成功破译了伏尼契手稿的部分内容的人之一，然而菲利甚至根本没有这份手稿的副本，他的所有工作都是基于纽博尔德教授和肯特的书中的插图！在所有这些研究者中，布伦博是一个值得注意的例外，因为他拥有在耶鲁大学工作这一优势，可以直接接触到伏尼契手稿的原本。

现在，伏尼契手稿的改写本已经可以在互联网上免费找到，也没有任何的法律限制。但是，在改写的过程中，某些信息被遗失了。比如，要把手稿中的文字和大量的插图对应起来并不容易。此外，我们甚至不清楚这份手稿的密码字母表中到底应该有多少种字符，可以看到，不同的研究者给出的改写字母表的字符数量完全不同。

任何针对这份手稿进行的统计检验都必须基于某种特定的字母表进

行。如果我们使用了错误的字母表，我们得到的结果就可能是毫无意义的。

在创造改写字母表的时候，我们遇到的问题之一是：手稿中有时候会出现一些高度相似的字符。比如说，、和这3个字符究竟是不是相同的字符呢？而、、和这4个字符又是不是同样的字符呢？我认为左上角的圈是一个非常重要的细节，因为这些字符中要么就是在左上角清楚地出现了一个圈，要么就是没有圈，而不存在任何中间的状态。也许，有没有这个圈的区别就相当于德语中u和ü之间的区别，或者o和ö的区别。

此外，还有一重困难。让我们来考虑这个字符，这究竟是一个字符还是两个字符呢？在你下结论之前，请注意伏尼契手稿中不仅存在这个字符，还存在和这样的字符。如果最开始的这一短斜线是一个字符，那么这份密码就不太可能是MASC密码，因为没有字母会连续重复出现3次。

此外，手稿中还存在这样一个字符：。上一段中提到的几个符号可能代表和它们样子类似的罗马数字，即 = ix = 9， = iix = 8， = iiix = 7。但是这个符号又代表什么意思呢？

在制定出一份改写字母表之前，我们还有许多问题需要讨论。雅克·盖伊（Jaques Guy）注意到，这个字符之后总是跟着一个上方有一条小横线的。而这种上方带有一条小横线的又总是出现在或者不带横线的之后。根据这一现象，盖伊判断和是单个字母。此外盖伊还注意到，手稿中经常出现，甚至也会不时出现，因此他判断代表单个字母。盖伊还认为和也很有可能代表单个字母。

在图1–24中，我列出了不同研究者以及两个研究小组所使用的改写字母表。这两个研究小组都是美国国家安全局组建的，第一个研究小组于1944—1946年期间进行了伏尼契手稿的破译工作，第二个研究小组在1962—1963年从事了相关工作。

表中的“基施尔”（Kirscher）看起来像是基歇尔的笔误。然而，我们在前文中已经说过，目前没有发现基歇尔对伏尼契手稿进行破译工作的任何证据。“基施尔”确实是一个笔误，但是它原本所指的不是基歇尔，而是杰弗里·克里舍尔（Jeffrey Krischer）。克里舍尔是一名具有数学、计算机科学、医学，以及密码学背景的研究者。他在哈佛大学读研究生时，曾对伏尼契手稿中的文字进行过计算机分析。

蒂尔特曼	第一研究小组	第二研究小组	基施尔	柯里尔	丁佩里奥
D H G 8 2 4 0 A C I T S L R E DZ HZ	P F H D G A R K 2 0 L N M 8 4 E C T S I PZ FZ HZ DZ V Y ' '' 0	4 0 9 8 2 B P V F # $ % @ S Z C A E I Y J U K G Q D N M W H L R T / — •	4	4 0 8 9 2 E R S Z P B F V Q W X Y A C I G H 1 T U 0 D N M 3 J K L 5 6 7 / — =	A B C D E F G H I J K L N O P Q R S T W X Y Z 2 1 3 6 7 8 9 0 space ( ) / ?
	space para ?	space line end ?	para start line start line end space	space line end para end	space line start line end para end ?

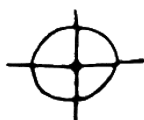
图1-24 几位手稿研究者给出的改写字母表

除了图1–24中的这些改写字母表以外，还有一份距今更近的字母

表，被称为“欧洲伏尼契字母表”（EVA）。这份字母表是由勒内·赞德伯根（René Zandbergen）和加布里埃尔·兰迪尼（Gabriel Landini）于1996—1997年总结出来的。此外，还有若干其他版本的改写字母表。

下面，我们来研究对几种改写字母表所做的统计检验。

元音辨认算法



我们可以用若干种算法来判断一段文字中的哪些字符最可能是元音字母。当然，这些测试只对MASC密码有效。也就是说，对于靠变换字母顺序或者其他更加复杂的加密方式产生的密码，上述算法就无法给出有意义的结果了。就我所知，元音辨认算法最早可以追溯到弗朗索瓦·维埃特（Francois Viete，1540—1603）。维埃特不仅研究了单个字符出现的频率，而且还研究了双字符以及三字符组合出现的频率。

所有元音辨认算法背后的基础原理都是：和辅音字母相比，元音字母可以与更多的字母结合在一起。让我们考虑元音字母A。我们几乎可以在字母A之后加上字母表内的任何字母。比如有以下这些词：AARDVARK、ABOUT、ACT、ADD、AERONAUTICS、AFTER等。但是，如果我们想在一个辅音字母——比如B——后面加上其他字母，就常常会遇到麻烦。BA开头的单词有BAR，但是如果要找BB开头的单词就找不到了，除非我们让BB出现在一个单词的中间，比如RUBBLE。如果考虑BC，也会遇到类似的问题。我想不到任何以BC开头的单词，即使允许BC出现在一个单词的中间，我也只能想到BOBCAT一词。但是BOBCAT一词事实上是由BOB和CAT两个词组成的合成词，因此这个单词实际上是人为地将B和C连在一起。如果你

试着寻找含有BD、BE、BF、BG、BH、BI、BJ、BK、BL等双字母组合的单词，你就会发现通常只有合成词。

因此，如果我们想要判断一个未知的字母究竟是元音字母还是辅音字母，我们只需要简单地统计一下与这个字母相邻的字母有多少种。如果某个字母比较“挑剔”，只能与少数其他字母相邻，那么这个字母就很可能是辅音字母，而与这个字母相邻的字母则很有可能是元音字母。反之，如果某个字母能与许多不同的字母相邻，那么这个字母就是元音字母。我们可以说，元音字母非常“热衷于社交”。有时候，我们会把元音字母称为“字母表中的荡妇”，因为它们几乎可以和任何其他字母组合在一起。

这种方法的唯一潜在困难是：辅音字母和元音字母之间的界限究竟在哪里？如果与某个未知字母相邻的字母种类既不多也不少怎么办？当然，如果我们知道这种MASC密码的明文是用何种语言写成的，那么我们就能知道这种语言中一共有多少个元音字母。在这种情况下，只要把所有未知字母按与之相邻字母的数目从高到低排列，然后选出排名靠前的字母就可以了——这种语言中有几个元音字母，就选取几个字母。然而，我们还可以通过一些更加复杂的方式来取得更理想的结果。

海伦·盖纳（Helen Gaines）创造出了一种简单的算法，称为“辅音线方法”。福斯特（Foster）将其描述如下[注]：

我们用A(I)和B(I)分别表示与字符I后方和前方与之相邻的不同字母的数量。如果字符I是一个元音字母，那么A(I)和B(I)应该都很大，而且A(I)和B(I)应该大致相等。福斯特发现，对$A + B$或者$A \times B$这两个量取最大值所得到的结果差异不大。

目前最优的元音辨认算法是苏霍京算法（Sukhotin’s Algorithm），它包括以下6个步骤[注]：

1. 统计每个字母与所有其他字母（包括它自己）相邻的次数，

把该统计结果放入一个n×n的矩阵中，其中n是字母表中的字母总数。[注]

2. 把上述矩阵主对角线上（从左上到右下）的所有数值设为0。

3. 假设所有字母都是辅音字母。把每一横行的数值分别相加，得到的和写在行的右侧。

4. 找到数值最大的一个横行，假设这个字母是元音字母。如果剩下的所有“辅音字母”行的总和都是非正数，则终止算法。

5. 找出每行“辅音字母”与新发现的这个元音字母相邻的次数，从该行的总和中减去这个次数的两倍。

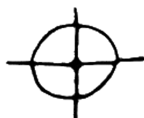
6. 回到第4步。

我在我的第一本书——《秘密的历史：密码学的故事》（*Secret History: The Story of Cryptology*）中更加详细地描述了苏霍京算法，并且还举了一个例子。有兴趣的读者可以阅读。

福斯特建议同时使用辅音线方法和苏霍京算法。这两种算法用计算机运行都很快，而且有两种测试可以进行能够让我们对测试的结论更有信心。此外，福斯特还研究了另一种方法，这种方法被称为“元音分布法”。这种方法的精确度不如以上两种算法，而且运算时间是以上两种算法的450倍（“元音分布法”大约耗时15分钟，而以上两种算法大约耗时2秒钟）。雅克·盖伊用他的字母表（该字母表包含17个字母）对伏尼契手稿的79v和80r两叶运行了苏霍京算法。苏霍京算法认为共有6个字母是元音字母，[注]这6个字母分别是：ᑕ、ᑕᑕ、o、9、a和ı。

我注意到o、a和ı看起来很像o、a和i，这是巧合吗？

无解的熵



由于伏尼契手稿中的文字结构性过强，所以手稿使用的不可能是比MASC密码更复杂的加密方式。更加先进的加密方式会让密文看起来更加随机，而一种完美的加密系统所产生的密文看起来则是完全随机的。但伏尼契手稿中的文字却表现出很强的秩序性。在伏尼契手稿中，某些字符组合经常出现，而某些字符组合则从未出现过。

事实上，我们可以通过一些非常简单的算法来对文字的秩序性（冗余度）或者非秩序性（也叫随机度或熵）建模。

为了解释这种算法的原理，让我们来看一些例子。考虑以下这段不完整的信息："I hate this job. I'm going to q…（我恨这份工作，我要……）"。如果我把这个句子再稍稍补全一些，比如告诉你下一个字母是u，那么你是否觉得这一提示能够向你传达更多的信息呢？也许你不会有这种感觉，因为在英语中字母u几乎总是跟在字母q之后。事实上，在这个句子中，接下来的几个字母都无法向读者提供太多新的信息。你可能猜到这个句子会以"quit（辞职）"结尾。当然，这个句子也可以以其他的词结尾。比如，整条信息也许写作："I hate this job. I'm going to query my boss about a raise.（我恨这份工作，我要找老板要求加薪。）"或者"I hate this job. I'm going to qualify for unemployment when my boss finally fires me.（我恨这份工作，等到老板把我炒掉之后，我就可以领取失业补助了。）"然而，上述这些可能性比这个句子以"quit（辞职）"一词结尾的可能性要低得多。

因此，评价一段文字的信息含量的主要依据是衡量文字中的每一部分能够被猜到，或者不能被猜到的程度有多高。能够被猜到的部分（或者说概率较高的部分）——比如字母q后面的字母可能是u——所包含

的信息较少。而不容易被猜到的部分（或者说概率较低的部分）则包含较多的信息。

我们可以用数学工具来进行上述评估。这个数学公式对于某些读者来说可能有些陌生，但是克劳德·香农（Claude Shannon）已经于20世纪40年代证明，这个公式是进行上述评估的唯一方式。香农的信息公式写作$-\log_2(M)$，其中M是信息的概率。如果一段文字可以自然地被分割为n个部分，那么这段文字所传递的总信息就是$-\sum_{i=1}^{n}\log_2(M_i)$，其中Σ是希腊字母西格玛，表示“求和”的意思。这个公式的意思是：我们应该把西格玛后面的算式针对i的每一个值累积相加。为了向读者说明这个问题，我举一个成绩单的例子。假设一张成绩单中包含4门不同课程的成绩。此处i可以取1、2、3、4这4个值，而这4门课的成绩是4条独立的信息：M_1、M_2、M_3和M_4。如果你认为自己在微积分课程中有80%的可能性能够得到A，并且确实得到了A，那么成绩单这部分文字的信息含量就是$-\log_2(0.8)$，约等于0.32。而如果你认为自己有95%的概率能够通过“街斗数学”[注]这门课[注]，然而你的成绩单却显示你不及格，那么这份成绩单的信息含量就是$-\log_2(0.05)$，约等于4.32——显著高于前一份成绩单的信息量。

负对数是一种很好的度量信息的方式，因为代入的数值（即概率）越小，得出的结果就越大。对于完全确定的信息（即概率等于1，也就是没有任何意外因素存在），对数给出的值为0，也就是说这一部分的信息量为0。此外，如果我们有两条信息M_1和M_2，我们就得到$-\log_2(M_1M_2) = [-\log_2(M_1)] + [-\log_2(M_2)]$，也就是说两条信息的总信息量等于各自信息量的和。我们希望上述所有这些性质成立，此外我们还希望，随着信息概率的变化，函数能够光滑地变化（即函数是连续的）。换句话说，我们不希望函数的值出现突然的跳动。香农证明，负对数是唯一能够满足上述这些性质的函数。我们可以改变对数的底（底不一定是2），然而这么做只不过是改变了度量的单位，或者可以说用不同的

比例尺来衡量同样的东西。因此，虽然比例尺可以进行改变，但是负对数是衡量信息量的唯一方法。

有了这样的数学公式，我们不仅可以度量一条或者多条消息的信息量，还可以衡量整个语言的信息量。为了达到上述目的，我们对这种语言中所有可能的消息的信息量进行加权平均。如果你熟悉“期望值”这个概念的话，你可以把这个结果理解为一个期望值。公式为：

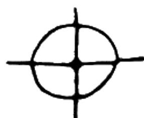
$$H = -\sum_{i=1}^{n} M_i \log_2(M_i)$$

在上述公式中，H表示这种语言的熵，M_i表示句子i的概率。比如，如果我们一共只有三个句子，这三个句子的概率分别是M_1、M_2、M_3，那么上述公式可以展开为：

$$H = -\sum_{i=1}^{3} M_i \log_2(M_i) = -[M_1\log_2(M_1) + M_2\log_2(M_2) + M_3\log_2(M_3)]$$

当然，实际上，某一种语言中有可能出现的消息的数量是极大的。想想你发送给朋友的短信有多少种可能性吧！如果我们计算出每一条消息的概率，然后再计算H的话，就会耗费很多时间。一种更加简单的方式是，我们可以只考虑单个字母的概率。我们把这称为“一阶熵”，一阶熵的计算公式为$H_1 = -\sum_{i=1}^{n} p_i \log_2(p_i)$，其中 p_i 是第i个字母出现的概率，而n是该语言中字母的总数。通过这种方法，就能得到H的估计值。当然，上述方法没有考虑字母组合带来的效应。如果想得到更准确的估计，我们可以在H_1以外再定义H_2、H_3等，也就是对双字母组合、三字母组合的概率进行求和。通过这种方法，我们就能掌握这种语言中两个相邻字母或者多个相邻字母之间的结构，比如在英语中，字母Q后面几乎一定跟着字母U，“字母E一定在字母I后面，除非E在字母C后面”等。随着n值的增大，H_n对H的逼近度也就越来越高。我们把H_2和H_3分别称为“二阶熵”和“三阶熵”。

冗余度计算



由于冗余度实际上就是混乱度或熵的反义词，所以我们可以根据熵值计算出冗余度的值。当所有字母出现的频率完全相等的时候，文字的熵就达到最大值，这时的文字就是完全随机的。我们把这个最大的熵值记作H_{max}。如果我们已经得到了一段文字的H值，并且想要知道H和H_{max}有多大的差距，我们就可以研究H和H_{max}的比值，即H/H_{max}。对于完全无序的文字而言，上述比例等于1，而对于冗余度很高的文字而言，上述比例则会接近于0。因此，如果我用1减去上述数值，这个结果就被反了过来。从某种意义上来说，这个结果（$1 - H/H_{max}$）给了我们一个关于语言冗余度的度量，我们通常用字母D来表示这个度量，即$D=1-H/H_{max}$。由于，$H_{max} = -\sum_{i=1}^{n}(1/n)\log_2(1/n) = -(1/n)\sum_{i=1}^{n}\log_2\left(\frac{1}{n}\right) = -(1/n)(n)\log_2(1/n) = -\log_2(1/n) = \log_2(1/n)^{-1} = \log_2(n)$，我们可以把$D$写作：$D = 1 - H/\log_2(n)$。

在上文中我们已经提到，为了对熵值进行更好的度量，我们可以考虑双字母组合和三字母组合，从而得到H_2和H_3。同样，我们也可以使用这些结果来获得对于冗余度的更好、更高阶的度量，即D_2和D_3。

现在，我们已经有了一种合理度量语言冗余度的方式，下面让我们来看看伏尼契手稿和各种不同语言之间的冗余度比较结果。但是，在我们进行这种比较之前，我们先应该搞清楚字母的定义是什么。在下面的数据中，我们都把空格视作一个字母。因为空格十分常见（出现的概率

很高），把空格视作一个字母所得到的冗余度会比忽略空格所得到的冗余度更高。如果我们只考虑英语字母表中的26个字母，而不考虑空格，那么英语的冗余度只有0.7左右。在之后的第5章，我们会用忽略空格所得的这种较低的冗余度来分析一个谋杀嫌疑人留下的密码。

表1-2 各种语言的冗余度

	冗余度[a]	
	D_1	D_2
英语	0.119	0.24
法语	0.131	0.27
德语	0.098	0.27
意大利语（军事用途）	0.127	0.20
西班牙语	0.132	0.26
日语（罗马拼音）	0.127	0.32
伏尼契手稿[b]	0.167	0.49

a：本表中的大部分值来自：Fischer, Elliot, “Language Redundancy and Cryptanalysis,” Cryptologia 3, no. 4 (October 1979).
b：我用以下文献中的H值来计算本表中的D值：Bennett, W.R., Scientific and Engine- ering Problem-Solving with the Computer (Englewood Cliffs, NJ: Prentice-Hall, 1976), 193.

从表1–2中，我们可以看到一个有趣的现象，那就是：各种自然语言的冗余度彼此相差很大。但是，伏尼契手稿的冗余度比上面列出的所有语言的冗余度都高出许多。也就是说，由于伏尼契手稿的冗余度过高，它不可能是用MASC密码加密的英语、法语、德语、意大利语、西班牙语或者日语。MASC密码虽然能够隐藏明文的信息，但却并不会改变明文的冗余度。

伏尼契手稿的冗余度过高，换种说法就是，这份手稿的熵值过低。

读者应该记得，熵值反映的是文字的无序程度，也就是冗余度的反面。

雅克·盖伊引用了贝内特（Bennett）的以下论点：“伏尼契手稿每个字符的平均熵值非常低，这个熵值低于目前任何语言中已经找到的正常文字。”[注]但是盖伊又指出，他认为贝内特的结果是没有意义的，因为贝内特把 和 这两个字符分别视作两个字母组成的字母对，而盖伊认为这两个字符代表的是单个字母。此外盖伊还指出，贝内特的分析中得到的伏尼契手稿的熵值和夏威夷语的熵值吻合。当然，我们没有理由认为伏尼契手稿的明文有可能是夏威夷语。各种语言（或著名作家所写文字）的熵值参见表1–3。[注]

表1-3 各种语言的熵值

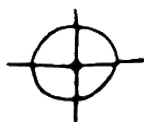
	H_1	H_2	H_3
英语			
现代英语	4.03	3.32	3.1
乔叟	4.00	3.07	2.12
莎士比亚	4.106	3.308	2.55
爱伦·坡	4.100	3.337	2.62
海明威	4.055	3.198	2.39
乔伊斯	4.144	3.377	2.55
德语	4.08	3.18	
法语	4.00	3.14	
意大利语	3.98	3.03	
西班牙语	3.98	3.01	
葡萄牙语	3.91	3.11	
拉丁语	4.05	3.27	2.38
希腊语	4.00	3.05	2.19
日语（川端康成）	4.809	3.633	
夏威夷语	3.20	2.454	1.982
伏尼契手稿（a）	3.66	2.22	

a：本表中的值基于伏尼契手稿的前10页，以及贝内特的字母表（包含21个字母）。

威廉·弗里德曼等一些研究者对伏尼契手稿和各种自然语言的熵值进行了上表中的比较。这些研究结果显示，伏尼契手稿的熵值非常低，甚至低到不像是一种真实的语言，除非这种语言是夏威夷语，或者某种

其他波利尼西亚语。弗里德曼并不认为伏尼契手稿是一个骗局，但他也不认为伏尼契手稿是用波利尼西亚语写成的。我们将在本章结尾继续讨论弗里德曼的理论。现在，我们先来看一看柯里尔上尉的研究成果。

柯里尔上尉的研究成果



1941年1月，一个四人代表团离开美国，前往英格兰，去完成一项极为重要的任务。此时，美国的密码专家已经破译了代号为“紫色”的日本外交密码，并且已经造出了能破解用这种密码加密的信息的解码机器，被称为“紫色模拟机”。这个私人代表团携带着一台这种模拟解码机，作为送给布莱奇利园的英国密码破译工作者的礼物。美国政府希望，也许在接受这份礼物以后，大洋彼岸的密码破译人员会和美国分享他们对纳粹密码的破译成果。在这个由四人组成的美国代表团中，两名代表来自陆军，另外两名代表来自海军。在这两名来自美国海军的代表中，就有一名是我们马上要讨论的密码专家：普雷斯库特·H.柯里尔（Prescott H.Currier）上尉。

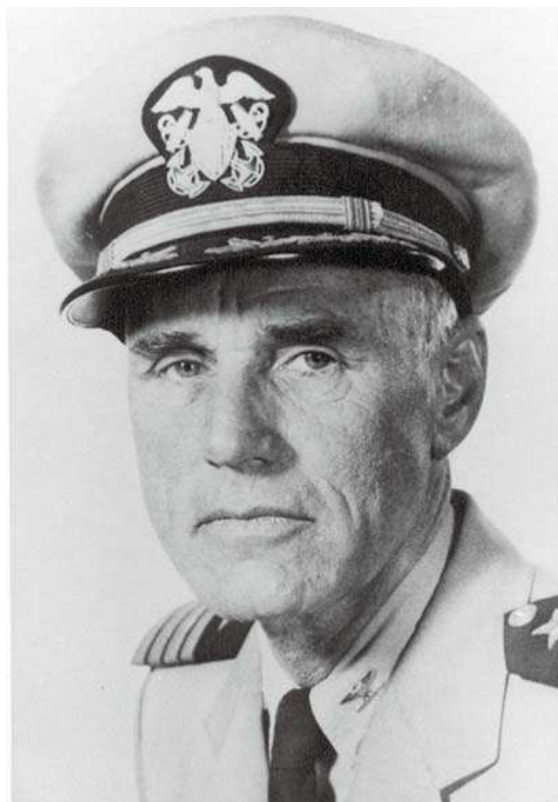


图1-25 普雷斯库特•H.柯里尔上尉

柯里尔能够和其他几名代表共同承担美国政府的这项级别极高的重要任务，说明当时他是一名极受重视的密码专家。我们稍后还会继续讨论美国代表团的这次任务，但是，现在让我们先暂时跳过战争时期，来看看和平时代发生的故事。在战争时期，这些密码专家只能破译敌方的密码，而在和平时代中，他们才可能有时间和精力去破译其他密码。

曾为美国陆军安全局（ASA）工作的技术史学家艾伯特·H.卡特（Albert H.Carter）教授于1946年判断，整份伏尼契手稿的笔迹是一致的。美国陆军安全局是美国国家安全局的前身组织之一。1976年，柯里尔作为美国国家安全局的一名分析师，提出了强有力的证据，证明卡特的上述结论是错误的。

柯里尔发现，在伏尼契手稿中，有两种不同的笔迹，分别代表两种不同的“语言”。柯里尔首先从伏尼契手稿的草本/植物学部分开始，他把从这部分开始所用的语言称为第一种语言，即语言A，这种语言共占据25个对开页。草本/植物学部分的后一半也有25个对开页，这25个对开页中包含两种笔迹，分别对应两种不同的语言。柯里尔把第二种语言称为语言B。在本章之前的部分中，我曾经用图表向读者展示过伏尼契手稿中单词长度的分布情况。事实上，那张表格展示的只是语言B中单词长度的分布情况。因此，在那张表格中我们将伏尼契手稿标记为“VMS B”。在柯里尔得到上述研究成果以后，我们就有理由把伏尼契手稿中的两种语言区别对待，并比较这两部分文字在统计性质上的区别了。

在伏尼契手稿的其他部分中，也出现了语言A和语言B。注意，在我第一次提到“语言”这个词的时候，我给这两个字加了引号，这是因为，在这里我说的“语言”并不是正常语境下的语言，我只是想借助“语言”一词来说明A部分和B部分在统计上是有区别的。柯里尔发现，伏尼契手稿的天文学部分没有表现出统计上的区别，他还发现生物学部分完全是用语言B写成的。药剂学部分的中段是用另一种语言写成的，并且这段的笔迹和药剂学部分开头以及结尾的笔迹不同。事实上，柯里尔发现“药剂学部分至少有4种不同的笔迹”。柯里尔认为，伏尼契手稿一共

有两种语言，但是执笔的人有若干名。

柯里尔给出了以下这些统计上的证据，来证明伏尼契手稿的草本/植物学部分中包含两种不同的语言。这些证据是：

1. 语言B中以89两个字符结尾的情况很多，而在语言A中则完全不存在这种情况。

2. 语言A中出现cı8oc卌和cı8o2这两种组合的情况很多，而在语言B中这两种组合出现的频率很低。

3. cı8aıı卄和cı8aı卄这两种组合在语言B中很少出现，而在语言A中出现的频率中等。

4. 以cı8oc卌卄组合开头的情况在语言A中较多，在语言B中极少。

5. 以c卌卄8组合开头的情况在语言A中较多，在语言B中较少。

6. 和前文不相连的末尾字符在语言B中随处可见，而在语言A中则较少。

更多详细的证据可以参见下图（图1–26）。该图复制自丁佩里奥所著的《伏尼契手稿——一个优雅的谜》（*The Voynich Manuscript — An Elegant Enigma*）一书。

虽然柯里尔发现手稿中的不同部分具有统计上的差异，但这些不同部分仍然可能是用同一种自然语言写成的，只是各部分使用了不同的技术术语，才导致了这种统计上的差别。如果我们相信手稿中的插图是有意义的，我们就能看出来伏尼契手稿涵盖的议题非常宽泛。

伏尼契符号	柯里尔 语言A （草本/植物学部分）	柯里尔 语言B （草本/植物学部分）	克里舍尔（103~116对开页）	丁佩里奥 （草本/植物学部分；天文学/占星术部分）
4	290	257	233	368
o	2249	1373	729	3389
8	884	1250	406	1333
9	1231	1529	464	1893
2	205	151	41	425
[illegible]	663	496	250	(all) 1005
[illegible]	531	495	201	(all) 971
[illegible]	1315	752	376	1373
[illegible]	415	289	93	557
[illegible]	516	376	187	734
[illegible]	75	108	47	154
[illegible]	595	801	267	865
[illegible]	21	63	6	53
[illegible]	165	51	13	266
[illegible]	42	12	7	49
[illegible]	86	100	15	106
[illegible]	7	9	2	29
a	900	1085	546	1470
c	769	1390	730	1094
[illegible]	16	8	2	[illegible] 216
[illegible]	4	1	0	[illegible] 835
[illegible]	1	0	0	[illegible] 167
[illegible]	0	0	0	[illegible] 23
[illegible]	22	45	35	[illegible] 689
[illegible]	8	24	11	[illegible] 12
[illegible]	3	2	1	[illegible] 2
[illegible]	38	3	4	[illegible] 0
[illegible]	82	73	38	[illegible] 7
[illegible]	455	286	153	[illegible] 3
[illegible]	18	22	0	[illegible] 36
[illegible]	78	99	23	[illegible] 13
[illegible]	6	5	1	
[illegible]	1	1	1	
[illegible]	0	0	0	
[illegible]	13	7	1	
[illegible]	5	5	11	
			[illegible] 2	
总计	11709	11168	4896	18137

图1-26 支持两种不同语言的更多统计证据

最终，研究者在伏尼契手稿中一共发现了12种不同的笔迹。[注]虽然这一发现似乎使问题变得更加复杂了，但它却帮助我们排除了关于手稿的一种可能性。如果这份手稿是由多位作者或者多位执笔者共同完成的，那么这份手稿就不太可能是一个精神错乱的人写出来的毫无意义的内容。当然，我们仍然不能排除骗局的可能性，笔迹的区别或许只不过说明这个骗局的作者不是一个人，而是多个人而已。

此外，柯里尔还发现，伏尼契手稿从头到尾都符合某些奇怪的统计学特征。比如，他发现，伏尼契手稿中的有些内容似乎是一些“功能性的内容”。柯里尔写道：“同一批字符，在句子开头和结尾的频率统计结果与在句子中的频率统计结果显著不同。比如，某些字符不会出现在一行的开头，而另一些字符作为一行的首个“单词”的第一个音节出现的频率大约为期望值的百分之一。”

根据柯里尔的说法，在伏尼契手稿中，一行的末尾经常包含一些无意义的符号，似乎作者在写完一行的时候加入了一些无用的信息。柯里尔把这些出现在句子结尾处的字符描述为“在手稿的其他地方不会出现的几个字母”。其中一个字符在手稿的其他部分中也出现过，但它出现在一行结尾的频率高达85%。由于我们不知道伏尼契手稿的字母表中究竟有多少个字母，这种不确定性使我们的统计结果不够可信，如果句子结尾的某些字符并不是手稿真正内容的一部分，它还会进一步降低上述统计测试结果的有效性。这样一来，我们可能需要重新分析伏尼契手稿中出现的这些字符，并且更加重视它们出现在句子开头和中间的情况。然而，后来有一位研究者尼克·佩林认为，在伏尼契手稿中，有一个符号（或者符号团）出现在一行结尾处的频率远远大于出现在其他部分的频率，因此可能代表的单词跨行时所使用的连字符。如果佩林的这种说法成立，那么也许句子结尾处经常出现这些奇怪的符号实际上是有意义的。

还有研究者指出了伏尼契手稿其他一些奇怪的统计特征。比如，在伏尼契手稿中，缺乏两个相同的字母连在一起的情况。当然，这种说法

忽略了 和 这两个符号，因为这些研究者认为，这两个符号各自代表单个的字符。

在前文介绍柯里尔的时候，我们提到他在第二次世界大战期间曾代表美国军方访问英国，执行一项重要的情报分享任务。现在我们要谈到的另一位密码专家则属于这次情报分享任务中的英国代表一方。



图1-27 约翰·蒂尔特曼准将（1894—1982）

约翰·蒂尔特曼（John Tiltman）在英格兰享有盛名，他被认为在破译手写密码方面“无人能及”。他曾于20世纪20年代破解过多种苏联密码系统，于20世纪30年代破解过日本的密码系统，于1939年和1940年破解过纳粹的战场密码。1940年夏天，蒂尔特曼在破解铁路恩尼格玛密码的工作中起到了重要作用。被破译出的一些信息显示，德军要在1941年把多个部队调往东线。这条情报和许多其他的迹象促使温斯顿·丘吉尔警告苏联，希特勒即将对苏联发起进攻。然而，斯大林似乎谁也不相信（或许他只相信希特勒），他并没有采纳丘吉尔的建议。

因此，当英国的情报机构需要决定是否与美方共享情报时，蒂尔特曼准将的个人意见是颇有一些分量的。当时，有些人担心，由于美方自己的加密系统比较薄弱，他们可能会无意间泄露英方好不容易取得的密码破译成果。然而，蒂尔特曼驳斥了这些反对的声音，他坚持认为英国政府应该与美国政府建立情报共享。美国国家安全局的密码历史中心发表的一份报告称：“蒂尔特曼的成功为一项史无前例的合作打下了基础，这种合作今天仍在继续。”[注] 1942年春天，英国政府首次与美国政

府共享情报，蒂尔特曼本人亲自乘坐美国的战舰横跨大西洋，为美国的密码专家送去了8个装满了报告和技术信息的沉甸甸的包裹。

随着第二次世界大战的进行，蒂尔特曼又积累了许多密码破译方面的成功经验。1942年，他成功破解出另一个日本密码系统，并且迈出了破解洛伦兹SZ40密码机的第一步。洛伦兹SZ40密码机在英国军方的代号是“金枪鱼”，这是阿道夫·希特勒用来与高级将领交换信息的密码机。随着德国的党卫队系统和警察系统被破译，盟军才了解到纳粹政府对犹太人进行大屠杀的暴行。如果没有这些密码专家的辛勤工作，大屠杀可能还会持续更长的时间。

在20世纪50年代、60年代和70年代，蒂尔特曼在密码破译方面接连取得成功。虽然关于他在这段时间中的工作的许多细节目前尚未解密，但是我们知道他至少破解了东欧以及第三世界国家所使用的手写密码。

美国国家安全局以及英国的政府通信总部都对蒂尔特曼做出的这些贡献给予了高度的肯定。美国国家安全局把蒂尔特曼的名字陈列在他们的名人堂之中，而英国政府通信总部的负责人布赖恩·托维（Brian Tovey）爵士则把蒂尔特曼称为英国历史上最伟大的密码专家之一。

那么，这位破译了苏联人、日本人，以及纳粹的密码的破译大师又怎么会被一份几个世纪之前作者不详的加密手稿难倒呢？

大约在1951年，美国密码专家威廉·弗里德曼把伏尼契手稿的问题告诉了蒂尔特曼，并引起了后者的注意。1958—1964年期间，蒂尔特曼在美国国家安全局工作，此后也继续担任美国国家安全局顾问。而弗里德曼刚好于1962—1964年之间在美国国家安全局内组织了破译伏尼契手稿的第二研究小组。

虽然在蒂尔特曼之前，各方研究者已经做了许多工作，但是蒂尔特曼仍然在伏尼契手稿中发现了一些新的重要特点。蒂尔特曼注意到，伏尼契手稿中包含一些特殊的字符组，这些字符组具有共同的特点：它们几乎只出现在句子的开头、中间，或者结尾。也就是说，这份手稿中包

含数量可观的前缀、词根，以及后缀。下表中列出了一些例子。这可能说明，伏尼契手稿是用一种综合语写成的。这些后缀出现于动词词根的后面时，可能表示人称变化、数的变化，也可能表示过去时、现在时和将来时的时态变化，还可能表示不定式。比如：

表1-4 关于后缀意义的一些例子

	第一人称	第二人称	第三人称
过去时	[illegible]	[illegible]	[illegible]
现在时	[illegible]	[illegible]	[illegible]
将来时	[illegible]	[illegible]	[illegible]

上表中的这些例子只是为了说明这些后缀的性质，这些具体的解法并不一定正确。而其他一些后缀，比如9和89，则可能表示名词的复数形式。

蒂尔特曼列出的后缀例子不够多，不能够完全对应大部分语言中的各种后缀形式。也许伏尼契手稿中还存在其他一些后缀形式，然而由于这些后缀只是零散地出现，所以很难从加密的手稿中提炼出来。但是也不能排除伏尼契手稿中确实没有使用其他后缀形式的可能性。比如，某些作者在提到自己的时候不喜欢使用“我”这个人称代词，而喜欢用“我们”。我在普林斯顿大学出版社的编辑恨透了这种写法！

除了前缀和后缀以外，蒂尔特曼还给出了一个常用词根的列表。

我在向读者介绍蒂尔特曼在密码方面的成就时，仅仅提到了他曾经破解的密码系统。需要补充的是，蒂尔特曼不仅善于破解密码，他还同样善于制造密码。蒂尔特曼制造的密码系统曾经给纳粹带来了许多麻烦。某些早期的英国加密系统先根据一个密码本把文字转化为数字，然后再在这些数字中加入一些数字作为一重额外的伪装。这些后加入的数字被称为“附加数”。添加附加数的最重要的指导原则是：附加数的随机

程度越高越好。如果这些附加数被重复使用，或者能够以某种方式被猜出来，那么敌人就有机会破解这个加密系统。蒂尔特曼对附加数表进行了如下改进：他将附加数表与一块“格栅”结合在一起使用。所谓“格栅”就是一块扁平的塑料板，在这块塑料板上的不同位置挖出许多小洞，透过这些小洞能看到100个4位附加数。只要把这块格栅在附加数表上移动，就可以挑选出不同的附加数组合。即使在有这个格栅的情况下，加密方也会每天更换附加数表。

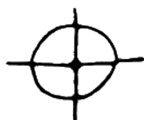
图1-28 出现在词头和词尾的一些常见的符号组

蒂尔特曼发明的这种格栅有一个官方的名字叫作“模板减法器框架”（Stencil Subtractor Frame，又称S.S.框架或者SSF）。英国于1943年12月引入了这种格栅。此前，在同年6月，英国还启用了一个新的密码

本。在添加了这两重加密之后，德军便无法破译英国海军的通信内容了。

然而，格栅还有另外一重用途。以此为基础，英国研究者戈登·鲁格（Gordon Rugg）在2004年提出了一种理论，认为伏尼契手稿完全就是一个骗局。

戈登·鲁格的理论



戈登·鲁格的理论认为，只要使用某种“音节”格栅，就可以创造出和伏尼契手稿中的文字具有相同统计性质的文字。这种音节格栅可参见图1–29。

有了这种格栅以后，只需要把它放在一个表格上，每次只显示出3个相邻竖列的音节就可以了。然后，加密者可以把这3个音节抄写到一张纸上，再移动格栅，挑选出另外3个音节，再把这3个音节抄下来。通过使用不同的格栅，并将这些孔洞位置不同的格栅放在表格的不同位置上，加密者就能够制造出许多文字。这些文字的结构性质与蒂尔特曼及其他研究者在伏尼契手稿中发现的性质是一样的。

鲁格进一步解释，运用这种方法，表格的大小可以有很多变化，格栅也不一定只能有3个孔洞。他所举的上面这个例子只是为了说明的方便而已。

柯里尔之所以会在伏尼契手稿中发现两种语言（即伏尼契语言A和伏尼契语言B），可能只是因为在手稿的不同部分中使用了两种不同的表格而已。

图1-29 一种可以用来创造假文字的格栅

那么，这个骗局的制造者究竟是谁呢？鲁格指出，约翰·迪伊和爱德华·凯利曾经用一种类似的方法创造出一种所谓的“天使”语言，叫作以诺语言（Enochian）。

锁定了两位嫌疑人之后，鲁格的理论听起来就更加有道理了。2007年，奥地利物理学家安德烈亚斯·申纳（Andreas Schinner）为鲁格的上述理论提出了更多支持性证据。申纳的这篇论文比鲁格的论文更注重技术，但殊途同归，得到了和鲁格同样的结论。为了满足对技术细节有兴趣的读者的需求，我将申纳的这篇论文的摘要列出：

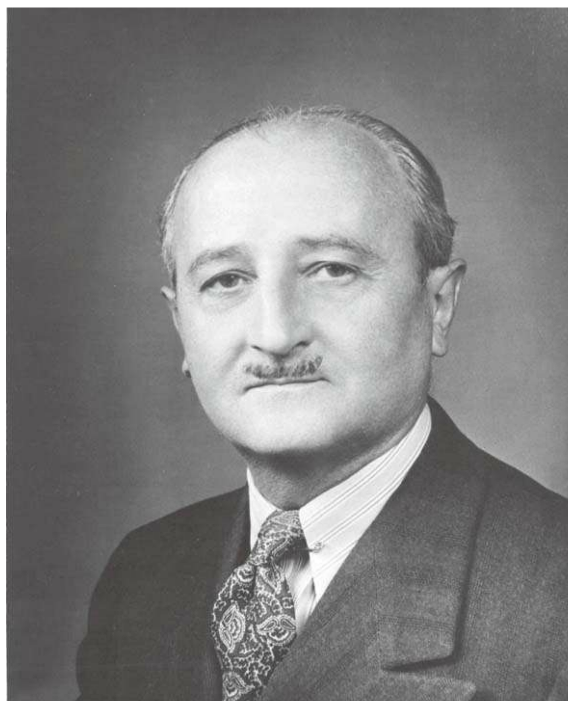
> 在这篇文章中，我将使用无规行走映射以及标志/音节重复统计的方法来分析伏尼契手稿。本文的研究结果将伏尼契手稿的可能解法的范围显著缩小。结果显示，伏尼契手稿的文字是通过一个随机过程产生的，而不是由某种语言加密而得到的。有了本文的研究成果以后，所谓的“中国理论”变得不再可信。㊟

在本章之前的内容中，我们已经看到了几种认为伏尼契手稿是骗局的理论。你是否觉得某种理论特别有道理呢？在过去几十年的时间中，关于这一点，顶级专家之间都产生了意见上的分歧。美国国家安全局的工作人员玛丽·E.丁佩里奥（她也曾经出版过一本关于伏尼契手稿的佳

作）也同意骗局理论，但是蒂尔特曼不接受。㊟

罗纳德·W.克拉克（Ronald W.Clark）曾于1972年出版过一本关于爱因斯坦的畅销书《爱因斯坦：生活和时代》（*Einstein: The Life and Times*）。也许是为了再创辉煌，克拉克一直希望再写一本关于其他天才人物的传记。1977年，克拉克出版了威廉·F.弗里德曼的传记。㊟

弗里德曼几乎就是美国版的蒂尔特曼，或者，你也可以说蒂尔特曼就是英国版的弗里德曼。两位都非常善于破译手写密码。为了纪念弗里德曼的成就，美国国家安全局以弗里德曼的名字命名了他们的大礼堂。此外，弗里德曼的名字也陈列在美国国家安全局的名人堂中。最近，美国国家安全局解密了52 000多页文字材料，都与弗里德曼的破译生涯有关。㊟在第二次世界大战之前以及战争期间，日本曾使用过代号为“紫色”的重要外交密码。这一密码系统后被美国成功破译，负责管理整个破译团队的人就是弗里德曼。此外，美国国家安全局几十年来一直用弗里德曼写的教科书对密码专家进行培训。甚至连“密码分析”（cryptanalysis）这个词都是由弗里德曼创造出来的。那么，关于伏尼契手稿，弗里德曼又得出了怎样的结论呢？



对于这个问题，弗里德曼并没有轻率地提出一些不成熟的结论。1944年5月26日（此时第二次世界大战仍在进行当中），弗里德曼在美国国家安全局成立了一个研究伏尼契手稿的研究小组。这个研究小组刚成立的时候共有16名成员。幸运的是，这16名密码专家只是在正常工作结束以后才聚在一起研究伏尼契手稿，他们并没有为了破译伏尼契手稿而忽略对德国和日本的密码系统的破译工作，毕竟后者才是他

们的本职工作。这个研究小组开始改写伏尼契手稿中的字符，并且把这些字符制作成穿孔卡片，以便用那个时代的计算机进行统计分析。虽然在1945—1946年期间，小组举行了多次会议，但他们并没有完成破译伏尼契手稿的工作。

图1-30 威廉•F.弗里德曼(1891—1969)

1962年9月25日，弗里德曼又成立了研究伏尼契手稿的第二研究小组。第二研究小组的工作目标和第一研究小组一样，都是完成对伏尼契手稿的全面改写和破译工作。但是，第二研究小组并没有在第一研究小组的基础上继续前进。在前文中展示了一份不同小组使用的改写字母表的对比图，从那张图中我们可以看出，第二研究小组使用的改写字母表和第一研究小组使用的改写字母表并不相同。到了1963年夏末，第二研究小组也停止了破译伏尼契手稿的工作。这次，破译的工作仍然没有完成。第一研究小组对伏尼契手稿做了大量的研究工作，足以形成一种观点。而第二研究小组所做的努力并没有改变上述观点。

西奥多·C.彼得森（Theodore C.Peterson）神父曾经为弗里德曼的研究小组提供过伏尼契手稿的影印版，使他们得以进行部分的改写破译工作。彼得森神父自己也对伏尼契手稿进行了令人惊叹的研究工作。他为伏尼契手稿做了一份词汇索引，就像《圣经》的词汇索引一样，你可以通过这份索引查到手稿中的每一个词出现的所有页码。此外，你还能从中查到与任何一个词相邻的词。通过这份词汇索引，我们发现伏尼契手稿具有一个非常奇怪的性质，那就是一个相同的词连续出现两次的例子非常多。

现在，让我们再把话题转到弗里德曼身上。弗里德曼发表了他关于伏尼契手稿的理论，但是他发表的这段内容用变换字母顺序的方法加密过。也就是说，弗里德曼通过变换一个句子中的字母顺序，把这个句子变成了另一个有意义的句子。弗里德曼的这一意见发表于1959年，此时第一研究小组的工作已经结束，而第二研究小组的工作还没有开始：

I put no trust in anagrammatic acrostic ciphers, for they are of little real value — a waste — and may prove nothing — Finis. (注)

（我完全不相信通过变换字母顺序创造出的藏头诗密码，因为这种密码没有什么真正的价值，完全是浪费时间，也不能证明任何事情——完毕。）

关于这段密文的明文究竟是什么，许多读者提出了各种不同的解法，比如：

William F.Friedman in a feature article arranges to use cryptanalysis to prove he got at that Voynich manuscript. No?

（威廉·F.弗里德曼在一篇专题文章中使用密码分析的方法来证明他已经破译了伏尼契手稿。不是这样吗？）

This is a trap, not a trot. Actually I can see no apt way of unravelling the rare Voynich manuscript. For me, defeat is grim.

（这是一个陷阱，而不是一个答案。事实上我找不到任何合理的方式来破译这份罕有的伏尼契手稿。对我来说，失败是残酷的。）

To arrive at a solution of the Voynich manuscript, try these general tactics: a song, a punt, a prayer. William F.Friedman.

（要想得到伏尼契手稿的解法，试试这种普通的方法：一首歌、一艘方头平底船、一段祈祷文。威廉·F.弗里德曼）

从上面这些不同的解法中，我们可以看出为什么纽博尔德对字母进

行随机重排的方式并不是一个好的解答途径！读者可能还记得，纽博尔德对每组55个字符或者110个字符进行了顺序重排。而弗里德曼的上述信息一共只有96个字符，就可以形成以上几种截然不同的解法了。

这段密文的正确解法于1970年被公布于世。此时，弗里德曼已经去世。正确的解法是：

> The Voynich MSS was an early attempt to construct an artificial or universal language of the a priori type. —Friedman. (注)
>
> （伏尼契手稿是用演绎的方式创造一种人工语言或者通用语的早期尝试。——弗里德曼）

几百年来，人们曾经多次研究过上述这种人工语言设计方案，这类方案有许多不同的名字，比如合成语言、人工语言，或者通用语。在前文中，我们曾经提到，基歇尔曾试图创造一种通用的书写系统，这就是人工语言的一个例子。然而，基歇尔并不是唯一一个想要完成这项工作的聪明人。微积分的发明人之一戈特弗里德·冯·莱布尼茨（Gottfried von Leibniz）也曾经试图创造出这样一种系统。此外，弗朗西斯·培根（Francis Bacon）爵士也同样进行过这方面的尝试。但是，弗里德曼认为，上述这几个人都不是这份加密手稿的作者，因为弗里德曼认为这份手稿的完成时间应该在1480—1520年之间，这几个人当时都还没有出生。

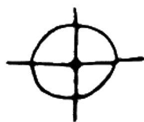
在上文中我们曾经提到，弗里德曼把伏尼契手稿的情况告诉了蒂尔特曼。也许，弗里德曼这样做是希望获得关于伏尼契手稿的另一个独立意见。结果，蒂尔特曼的意见与弗里德曼的意见一致。当来自英国和美国的密码巨头都得到了相同的结论时，我们显然有理由认真地对待他们得到的结论！

关于伏尼契手稿中使用的究竟是什么类型的人工语言，弗里德曼做

了非常具体的描述。弗里德曼写道：这种语言是一种“演绎型”的人工语言。在这类人工语言中，所有东西都被分成不同的门类，在每一种门类中又继续分为许多子门类。于是，在这种方法下，某个具体的词汇会写作$x_1x_2x_3y$的形式。其中各个x表示这些门类和子门类；而y是一个表示结束的符号，用于完结这部分文字。前文中已经说过，蒂尔特曼在伏尼契手稿中发现了多个前缀和后缀，这种演绎型人工语言的理论正好能解释上述现象。这种语言的结构与世界上自然产生的语言结构完全不同，甚至与基于真实语言的模式创造出来的人工语言的结构也完全不同。

虽然弗里德曼于1969年去世，但是美国国家安全局对于伏尼契手稿的兴趣并没有就此终结。美国国家安全局的一位分析师玛丽·丁佩里奥曾于1972年主持召开过一次伏尼契手稿研讨会。丁佩里奥所写的专题著作《伏尼契手稿——一个优雅的谜》于1976年出版，书中对迄今为止各种研究伏尼契手稿的工作进行了非常好的总结。然而，在此后的另一部关于伏尼契手稿的书中，作者质疑丁佩里奥“究竟是不是一个真实的人，还是美国国家安全局造出来的假名”。[注]这本书的作者宣称，除了与上述书稿的联系以外，他们无法找到关于丁佩里奥的任何信息，这样的情况使得他们不得不怀疑玛丽·丁佩里奥是一个假名。然而，她确实是一个真实存在的人。美国国家安全局的历史学家戴维·哈奇（David Hatch）曾说：“她再也没有机会公开发表任何著作了。因为在那个时代，美国国家安全局的雇员就像古典社会的淑女一样，在他们的一生中，公众只能听到他们的名字三次。[注]”[注]

伏尼契手稿的多个版本



1991年，吉姆·吉洛格利（即前文提到的詹姆斯·吉洛格利，昵称吉姆，他是一名计算机科学家和一位杰出的密码专家，在本书接下来的若干章节中，我会提到他几次）和吉姆·里兹（Jim Reeds，当时在贝尔实验室工作）将加密手稿研究方面的合作扩展到了互联网上。他们的第一步是创建了一个关于伏尼契手稿的电子邮件讨论组。里兹还整理出了关于伏尼契手稿历史背景知识的极为详细的资料。本章的参考文献以及延伸阅读列表都是以里兹整理的这些背景知识为基础的，在引用之前已征得了他的同意。

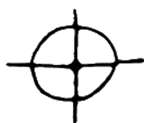
2004年，我们又迎来了一件更加令人兴奋的事。一本关于伏尼契手稿历史的书出版了，标题为《伏尼契手稿》（*The Voynich Manuscript*），其美国版和英国版使用了不同的副标题。这本书的作者是格里·肯尼迪（Gerry Kennedy）和罗布·邱吉尔（Rob Churchill）。自1978年布伦博的相关书籍出版以来，这还是第一本关于伏尼契手稿的大部头（除了各式各样的所谓“解法”之外）。接着，2005年又出版了一本关于伏尼契手稿的书：劳伦斯和南希·戈德斯通（Lawrence and Nancy Goldstone）的《修士与密码》（*The Friar and the Ciper*）。尼克·佩林是一名博客作者，专门写关于尚未解开的密码的内容，[注]他也于2006年出版了关于伏尼契手稿的书，书名叫《伏尼契的诅咒》（*The Curse of the Voynich*），但是这本书的印刷量比前两本书要小很多。

2011年，碳–14测年法显示，伏尼契手稿所使用的皮纸的制造年代应该在1404—1438年之间[注]。此时，距离伏尼契首次向公众宣告他发现这份手稿已经有将近100年的时间了。麦克龙研究院的研究显示，伏尼契手稿上的墨水的制造年代稍稍晚于皮纸的制造年代。[注]但是，克劳斯·施梅（Klaus Schmeh）说，他与格雷格·霍金斯（Greg Hodgins，用碳–14测年法进行鉴定的放射性碳专家）讨论过，霍金斯表示，无法判断墨水究竟是什么时候被写到皮纸上去的。多家媒体报道称，人们已经用科学方法鉴定出了墨水写到皮纸上的时间，但根据霍金斯的说法，这种说法是错误的。

此前，很多人都希望罗杰·培根是伏尼契手稿的作者，然而对皮纸制造日期的鉴定结果已经（基本）否认了这种假说。虽然罗杰·培根本人不可能是这份手稿的执笔者，但是上述假说的坚定支持者仍然可以坚持说，这份手稿的作者仍是罗杰·培根，只不过手稿的内容后来由其他人重新抄写而成罢了。

如果伏尼契手稿上的墨水确实在如此早的时间就被写到了皮纸上，我们就可以排除某些认为手稿系伪造的理论。虽然伏尼契手稿仍有可能是一份毫无意义的伪造品，但是这份手稿不可能是约翰·迪伊或者其他同时代的人为了愚弄鲁道夫二世而特意制造出来的。同样，虽然此前很多人怀疑这份手稿是威尔弗里德·伏尼契伪造的，但是有了碳–14测年法的鉴定结果以后，显然这种可能性也被排除了。即便这份手稿是某个骗子制造出来愚弄他人，并骗取钱财的，这个骗子也必须生活在15世纪。

展望未来

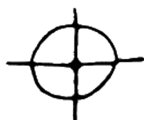


如果未来有人能找到伏尼契手稿的真正答案，一定会让公众极为兴奋。这种情况还是有可能出现的。尽管许多伟大而有智慧的人都失败了，但这并不代表破译伏尼契手稿是一件完全不可能的事，因为我们仍有可能找到能大幅推进破译工作的新信息。伏尼契手稿中缺失的那些书页在经历几个世纪以后是否可能仍然存在呢？这些缺失的书页可能是伏尼契之前的某个拥有者从原稿上取走的，而其中所包含的信息也许正是我们需要的。还有一个很自然的问题是：虽然我们尚未找到这份手稿的作者，但是这位作者有没有可能写过其他著作呢？我们很难相信这份既长，又复杂的手稿是该作者的第一部作品。如果能够找到该作者（们）

此前的作品，就可能为伏尼契手稿的破译工作带来一些启发。

1967年，戴维·卡恩（David Kahn）曾描述伏尼契手稿是“所有历史密码中最长、最广为人知、最诱人、被研究次数最多、最难破解以及最昂贵的一种”。[注] 50多年过去了，我相信直到今天，伏尼契手稿在历史密码中的地位仍然未被取代。

例文密码答案



His Majesty is interested only in wizards, alchymists, kabbalists and the like, sparing no expense to find all kinds of treasures, learn secrets and use scandalous ways of harming his enemies ... He also has a whole library of magic books. He strives all the time to eliminate God completely so that he may in future serve a different master.

（国王陛下只对巫师、炼金术士、犹太教神秘主义者这类人感兴趣，他不惜一切代价寻找宝藏、挖掘秘密，或用一些恶毒的方式打击他的敌人……

国王陛下的图书馆满是关于魔法的书籍。他无时无刻不在努力摆脱上帝的影响，这样他才好在未来追随其他的主宰者。）

字母替换规则表如下：

ABCDEFGHIJKLMNOPQRSTUVWXYZ（明文）

BFVDRQOGNUMJLYKSZIXHTEACWP（密文）

---

1. 1英寸≈2.54厘米。——编者注

2. E-mail received by the author on November 21, 2014. Also see http://en.wikipedia.org/wiki /Jerusalem_artichoke.

3. Newbold included the section I labeled “cosmological” as part of the biological section. See New-bold, W.R., “The Voynich Roger Bacon Manuscript.” Transactions of the College of Physicians and Surgeons of Philadelphia (1921): 431–74 (the relevant pages here are 461–63). Read April 20, 1921. Also see Newbold, W.R., and Kent, R..G., The Cipher of Roger Bacon, 1928, pp..44 and 46. Brumbaugh labels the sections as 1. Botanical, 2..Astrological, 3. Medical (perhaps dealing with human reproduction), 4. Medicinal, and 5..Appendix or Postscript. See Brumbaugh, Robert S., “Science in Cipher,” pp..109–41, in Brumbaugh, Robert S.(ed.), The Most Mysterious Manuscript, 1978, p. 110 cited here.

4. Six are suggested, for example, in Reddy, Sravana, and Kevin Knight, “What We Know about the Voynich Manuscript,” in Proceedings of the 5th ACL-HLT Workshop on Language Technology for Cultural Heritage, Social Sciences, and Humanities, pp..78–86, Portland, OR, June 24, 2011. Available online at http://www.aclweb.org/anthology/W11-1511 and https://www.aclweb .org/anthology/W/W11/W11-15.pdf.

5. “人所做的恶事在身后流传不绝，他们的美善良知却常跟着遗骨埋入坟墓。”语出莎士比亚的历史剧《恺撒大帝》。——译者注

6. Taken from Act 3, Scene 2 of William Shakespeare’s play Julius Caesar. This line is delivered by Marc Antony.

7. IRON MAIDEN意为“铁娘子”，是欧洲中世纪的一种刑具。——译者注

8. The quote was taken from Evans, R.J.W., Rudolf II and His World: A Study in Intellectual History 1576–1612 (Oxford: Clarendon Press, 1973), 196.

9. 在样本足够大的情况下，频率所趋近的值被称为概率。在这本书中，我们把一段密码中某个字母出现次数占总字母数的比率称为频率，而特定语言中某个字母出现的频繁程度则称为概率。——编者注

10. APP意为智能手机或电脑上的应用软件（“application”的缩写），是21世纪以来才流行起来的新词。——译者注

11. Code penguin, http://tools.codepenguin.com/patterns/help#.

12. Evans, Rudolf II and His World, 58.

13. Evans, Rudolf II and His World, 198.

14. Evans, Rudolf II and His World, 230. Also see Mukherjee, Ashoke, “Giordano Bruno, An Ever-Burning Flame of Commitment to Truth and Reason,” Breakthrough 8, no. 4 (2000):.1–13,available online at http://breakthrough-india.org/archives/bruno.pdf.

15. Evans, Rudolf II and His World, 279.

16. Stolfi, Jorge, Voynich Manuscript stuff, 2005, http://www.dcc.unicamp.br/stolfi/voynich/.

17. The graph is taken from Reddy and Knight, “What We Know,” p. 4. Available online at http:// www.isi.edu/natural-language/people/voynich-11.pdf.

18. Reddy and Knight, “What We Know,” 4, footnote.

19. This translates to “On the Secret Workings of Art and Nature, and on the Vanity of Magic.” Newbold, “The Voynich Roger Bacon Manuscript,” p. 456 cited here.

20. Kennedy, Gerry, and Rob Churchill, The Voynich Manuscript: The Unsolved Riddle of an Extraor-dinary Book Which Has Defied Interpretation for Centuries, British hardcover edition, Orion Books, London, 2004, p. 20, which, in turn, took it from Bacon, Roger, Compendium Studii Philosophiae, 1271 or 1272.

21. Some sources give a death date two years later. See, for example, Kennedy and Churchill, The Voynich Manuscript, p. 21. At http://www.nndb.com/people/582/000114240/ a death date of 1294 is conjectured, although uncertainty is expressed. Also see Newbold, “The Voynich Roger Bacon Manuscript,” 445–46, for the 1292 death date.

22. Lieutenant Colonel H.W.L.Hime, Royal Artillery, “Roger Bacon and Gunpowder,” pp..321– 36 in Roger Bacon Essays Contributed by Various Writers on the Occasion of the Commem-oration of the Seventh Centenary of His Birth, collected and edited by A.G.Little, Clarendon Press, Oxford, 1914, available online at http://archive.org/stream/rogerbaconessays00litt /rogerbaconessays00litt_djvu.txt. Also see Goldstone, Lawrence, and Nancy Goldstone, The Friar and the Cipher: Roger Bacon and the Unsolved Mystery of the Most Unusual Manuscript in the World (New York: Doubleday, 2005), 107–8.

23. Thorndike’s argument does not get into the details of the cipher itself. See Thorndike, Lynn, “Roger Bacon and Gunpowder,” Science, New Series 42 , no. 1092 (December 3, 1915): 799–800. This piece was reprinted as Appendix II (pp..688–91) of Thorndike’s A History of Magic and Experimental Science during the First Thirteen Centuries of our Era, Vol. II (New York: Columbia University Press, 1923), which is available online at https://archive.org/details /historyofmagicex02thor. The controversy is also mentioned in Goldstone and Goldstone, The Friar and the Cipher, 251.

24. Newbold, “The Voynich Roger Bacon Manuscript,” p. 457 cited here. Newbold noted that

this isn’t what Ethicus actually did, at least not in the ciphers of his that are known today.

25. Newbold, “The Voynich Roger Bacon Manuscript,” p. 456 cited here.

26. Newbold, “The Voynich Roger Bacon Manuscript,” p. 457 cited here.

27. Roberts, R.J., and A.G.Watson (eds.), John Dee’s Library Catalogue (London: The Bibliograph-ical Society, 1990).

28. Kennedy and Churchill, The Voynich Manuscript, 2004, p. 66, citing Prinke’s online article. Images comparing known samples of Dee’s numbers to those on the manuscript pages are provided on p. 67 of Kennedy and Churchill. Also see Pelling, Nick, The Curse of the Voynich: The Secret History of the World’s Most Mysterious Manuscript (Surbiton, Surrey, UK: Compelling Press, 2006),.11–13.

29. Goldstone and Goldstone, The Friar and the Cipher, pp..187–88. When Sir Francis Walsingham received intercepted messages penned by the imprisoned Mary, Queen of Scots, and conspir-ators planning to set her free and assassinate Queen Elizabeth, he likely had much confidence that the plaintexts could be recovered. It was his cryptanalyst Thomas Phelippes who suc-ceeded in breaking them, and the rest is history. Simon Singh’s The Code Book (New.York: Doubleday, 1999) does an excellent job of recounting this tale and the consequences for Mary (see chapter 1). Thomas Phelippes was also at a meeting of Walsingham and Dee. See Gold-stone and Goldstone, The Friar and the Cipher, 204–5.

30. Fell-Smith, Charlotte, John Dee (1527–1608), (London: Constable & Co. Ltd., 1909), 311. Avail-able online at https://archive.org/details/cu31924028928327.

31. Kelley was blackmailed by Sir Francis Walsingham into becoming a spy.

32. Brumbaugh, Robert S., editor and contributor, The Most Mysterious Manuscript: The Voynich “Roger Bacon” Cipher Manuscript (Carbondale, IL: Southern Illinois University Press, 1978),131.

33. I learned of this in Pelling, The Curse of the Voynich, p. 158, where credit for the discovery of the numbering system is given to Allan Wechsler and Ivan Derzhanski, who came upon it in-dependently.

34. Shelfmark APUG 557, fol. 353.

35. Translation taken from http://www.voynich.net/neal/barschius_translation.html, which incor-rectly dates it as 1637, the date of a previous letter that we do not have. The original Latin may be found at http://www.voynich.nu/letters.html#gb39, along with other letters connected with the manuscript.

36. 俄狄浦斯是猜出斯芬克斯谜题的人。——译者注

37. The text of this letter appears in Goldstone and Goldstone, The Friar and the Cipher,

pp..237– 39 and elsewhere.

38. Identified as “Dr Raphael Missowsky, Attorney General to Ferdinand III” in Kennedy and Chur-chill, The Voynich Manuscript, 73.

39. Kircher, Athanasius, The Volcanos: Or Burning and Fire-Vomiting Mountains, Famous in the World (London: J.Darby,1669): 35.

40. Goldstone and Goldstone, The Friar and the Cipher, 239.

41. Goldstone and Goldstone, The Friar and the Cipher, 239–40.

42. Voynich, Wilfrid M., “A Preliminary Sketch of the History of the Roger Bacon Cipher Manu-script.” Transactions of the College of Physicians of Philadelphia 43, ser. 3 (1921): 415–30. Read April 20, 1921.

43. Voynich, “A Preliminary Sketch.”

44. Voynich, “A Preliminary Sketch.”

45. Voynich, “A Preliminary Sketch.”

46. Voynich, “A Preliminary Sketch.”

47. Voynich, “A Preliminary Sketch.”

48. Sowerby, E.Millicent, Rare People and Rare Books (London: Constable & Co., Ltd, 1967).

49. Sowerby, Rare People and Rare Books.

50. Taratuta, Evgeniya, “Our Friend Ethel Lilian Boole/Voynich.” Moscow, 1964, translated from the Russian by Séamus ó Coigligh with additional notes, 2008.

51. Orioli, Giuseppe, Adventures of a Bookseller (New York: Robert M.McBride & Co., 1938).

52. Sowerby, Rare People and Rare Books.

53. Taratuta, “Our Friend Ethel Lilian Boole/Voynich.”

54. 1英里 ≈ 1.61千米。——编者注

55. Manly, John M., “The Most Mysterious Manuscript in the World.” Harper’s Monthly Magazine,143 (July 1921): 186–97.

56. Newbold, “The Voynich Roger Bacon Manuscript.”

57. Newbold, “The Voynich Roger Bacon Manuscript.”

58. Newbold, “The Voynich Roger Bacon Manuscript.”

59. Newbold, “The Voynich Roger Bacon Manuscript.”

60. Newbold, “The Voynich Roger Bacon Manuscript.”

61. Newbold, “The Voynich Roger Bacon Manuscript.”

62. Newbold, “The Voynich Roger Bacon Manuscript.”

63. Newbold, “The Voynich Roger Bacon Manuscript.”

64. Newbold, “The Voynich Roger Bacon Manuscript.”

65. Newbold, “The Voynich Roger Bacon Manuscript.”

66. Newbold, “The Voynich Roger Bacon Manuscript.”

67. Newbold, “The Voynich Roger Bacon Manuscript.”

68. Newbold, William Romaine. The Cipher of Roger Bacon, edited with foreword and notes by Roland Grubb Kent. (Philadelphia: University of Pennsylvania Press; London, H.Milford, Oxford University Press, 1928).

69. Newbold, “The Voynich Roger Bacon Manuscript.”

70. Bird, J.Malcolm, “The Roger Bacon Manuscript Investigations into Its History, and the Efforts to Decipher It.” Scientific American Monthly, June 1921, 492–96.

71. Anonymous, “The Roger Bacon Manuscript, What It Looks Like, and a Discussion of the Proba-bilities of Decipherment.” Scientific American, May 28, 1921, 432, 439–40.

72. Anonymous, “The Roger Bacon Manuscript.”

73. Thorndike, Lynn, “Roger Bacon.” The American Historical Review 34, no. 2 (January 1929): 317–19.

74. Manly, John Matthews., “Roger Bacon and the Voynich Manuscript.” Speculum 6 (July 1931): 345–91.

75. Manly, “Roger Bacon and the Voynich Manuscript.”

76. Manly, “Roger Bacon and the Voynich Manuscript.”

77. Manly, “Roger Bacon and the Voynich Manuscript.”

78. Manly, “Roger Bacon and the Voynich Manuscript.”

79. This name is hard to make out in the letter and may not have been reproduced correctly here.

80. “The Quirinal” refers to the Italian government of the time, so-called in reference to Quirinal Palace, which was used by kings, as well as being one of the homes of the presidents who fol-lowed them.

81. Also known as Peter and Pieter.

82. “蒙席”（Monsignor）是天主教会颁给有功神职人员的荣誉称号。——译者注

83. Kraus, H.P., A Rare Book Saga (New York: G.P.Putnam’s Sons, 1978), 222.

84. Thanks to Klaus Schmeh for pointing many of these out. He wrote, “Regarding the Voynich man-uscript alone, more than 15 ‘solutions’ are known to me, and all have turned out to be false.” See Schmeh, Klaus, “The Pathology of Cryptology — A Current Survey,” Cryptologia, 36, no. 1 (January 2012): 14–45. By the end of 2015, he was aware of more than thirty false solutions.

85. Strong, Leonell C., “Anthony Askham, the Author of the Voynich Manuscript.” Science, New Series 101, no. 2633 (June 15, 1945): 608–9.

86. Goldstone and Goldstone, The Friar and the Cipher, p. 276. The decipherment also included a “recipe for an herbal contraceptive.”

87. Brumbaugh, R.S.“The Solution of the Voynich ‘Roger Bacon’ Cipher.” Yale University Library Gazette 49, no. 4 (April 1975): 347–55. Brumbaugh later claimed that he found the solution in 1972, but he didn’t explain why no results were published until 1974. See Brumbaugh, R.S., “The Voynich ‘Roger Bacon’ Cipher Manuscript: Deciphered Maps of Stars.” Journal of the Warburg and Courtauld Institutes 39 (1976): 139–50.

88. Brumbaugh, “The Solution of the Voynich ‘Roger Bacon’ Cipher.”

89. Child, James R.“The Voynich Manuscript Revisited.” NSA Technical Journal 21, no. 3 (Summer 1976): 1–4.

90. Child, J.R., “Again, the Voynich Manuscript.” 2007. http://web.archive.org/web/20090616205410/http://voynichmanuscript.net/voynichpaper.pdf.

91. Goldstone and Goldstone, The Friar and the Cipher, 285.

92. 诺斯特拉达穆斯是16世纪的一名法国占星术士。——译者注

93. Finn, James E., “The Voynich Manuscript. Extraterrestrial Contact during the Middle Ages?”January 14, 2001. http://www.bibliotecapleyades.net/ciencia/esp_ciencia_manuscrito02.htm. Accessed March 23, 2015.

94. Zbigniew Banasik’s Manchu theory can be found online at http://www.ic.unicamp.br/~stolfi/voynich/04-05- 20-manchu-theo/ and at the links contained therein.

95. 布莱奇利园是“二战”时英国政府进行密码破译工作的主要地点。——译者注

96. Kennedy and Churchill, The Voynich Manuscript, 242.

97. Geheimnisvollstes Manuskript der Welt entschlüsselt, press release, 2005. Available online at http://www.ms408.de/downloads/Pressemitteilung.pdf.

98. http://www.ms408.de/context_d.htm.

99. http://www.edithsherwood.com/voynich_decoded/.

100. https://web.archive.org/web/20090609075537/http://www.voynich.nl/.

101. http://www.ciphermysteries.com/2009/11/12/richard-rogers-voynich-theory.

102. Watson, Leon, "Prophet of God" claims mysterious manuscript's code has been cracked,December 3, 2011, http://www.dailymail.co.uk/news/article-2069481/Prophet-God-claims-mysterious-manuscripts-code-cracked.html.

103. Watson, "Prophet of God."

104. Watson, "Prophet of God."

105. https://stephenbax.net/?page_id=11.

106. http://www.livescience.com/43542-voynich-manuscript-10-words-cracked.html.

107. http://theworldsfairest.com/writtenintongues/Written.in.Tongues-The.Voynich.Manuscript.Solved.pdf.

108. http://www.proza.ru/2015/01/11/2343.

109. Foster, Caxton C., "A Comparison of Vowel Identification Methods," Cryptologia 16, no. 3 (July 1992): 282–86.

110. An executable version of this algorithm can be downloaded from http://sun1.bham.ac.uk /G.Landini/evmt/evmt.htm. It's called VFQ and was written by Jacques Guy. The details of the algorithm are taken here from G.T.Sassoon, "The Application of Sukhotin's Algorithm to Certain Non-English Languages," Cryptologia 16, no. 2 (April 1992): 165–73.

111. This matrix is symmetric — although it mistakenly isn't in the example given in G.T.Sassoon, "The Application of Sukhotin's Algorithm to Certain Non-English Languages," Cryptologia 16, no. 2 (April 1992) 165–73.

112. Jacques Guy, "Statistical Properties of Two Folios of the Voynich Manuscript," Cryptologia 15, no. 3 (1991). The previous issue of Cryptologia (Jacques Guy, "Voynich Revisited" (letter to the editor), Cryptologia 15, no. 2, (April 1991)) contains a letter to the editor from Guy in which he claims that Sukhotin's algorithm resulted in only four vowels, but he did qualify that "not having kept my notes, [I] am quoting mostly from memory."

113. 麻省理工学院2008年确实开过一门名为"街斗数学"（Street-Fighting Mathematics）的课程。——编者注

114. This course was actually offered by Sanjoy Mahajan at MIT in 2008. See http://ocw.mit.edu /courses/mathematics/18- 098-street-fighting-mathematics-january-iap-2008/.

115. Guy, "Voynich Revisited" (letter to the editor), p. 162 quoted here.

116. Values taken from William Ralph Bennett, Jr., Scientific and Engineering Problem-Solving with the Computer, (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1976), 140, 193, and 194.

Missing val-ues in the third column simply hadn't been computed at the time this book was published.

117. Gerry Kennedy and Rob Churchill, The Voynich Manuscript: The Unsolved Riddle of an Extraor-dinary Book Which Has Defied Interpretation for Centuries, British hardcover edition, (London: Orion Books, 2004), 142. Pictures of seven different handwritings used in the manuscript appear on pp. 144–45. Currier originally estimated somewhere between six and eight different scribes.

118. John F.Clabby, Brigadier John Tiltman: A Giant among Cryptanalysts (Fort Meade, MD: Center for Cryptologic History, National Security Agency, 2007), 34.

119. Andreas Schinner, "The Voynich Manuscript: Evidence of the Hoax Hypothesis," Cryptologia 31, no. 2 (April 2007): 95–107.

120. D'Imperio, M.E.The Voynich Manuscript — An Elegant Enigma (Fort Meade, MD: National Security Agency, 1976). Reprinted by Aegean Park Press, Laguna Hills, CA, 1978.

121. Clark also published a biography of Edison that same year.

122. https://www.nsa.gov/public_info/declass/friedman_documents/.

123. W.F.Friedman and E.S.Friedman, "Acrostics, Anagrams, and Chaucer," Philological Quarterly 38 (1959): 1–20.

124. C.A.Zimansky, "William F.Friedman and the Voynich Manuscript," Philological Quarterly 49, no. 4 (1970): 433–42.

125. Lawrence Goldstone and Nancy Goldstone, The Friar and the Cipher: Roger Bacon and the Unsolved Mystery of the Most Unusual Manuscript in the World (New York: Doubleday, 2005), 284.

126. 西方有一个说法：对于一位淑女而言，在她的一生中，公众只能有三次机会在报纸上看到她的名字，那就是在她出生时、她结婚时，以及死亡时。——译者注

127. E-mail from David Hatch to the author, received July 6, 2015.

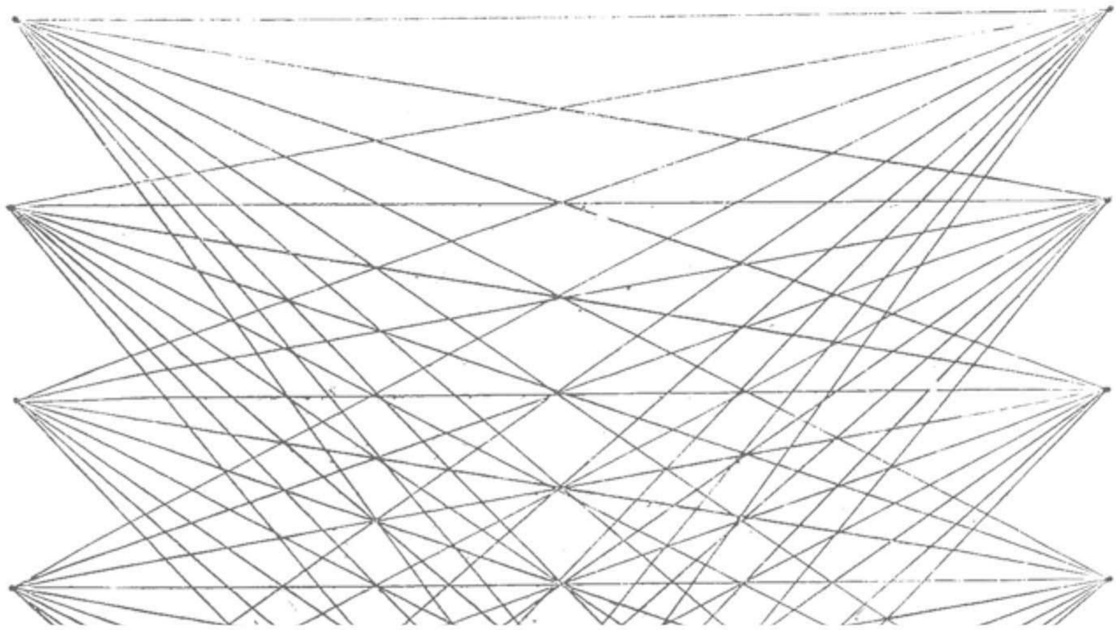
128. http://www.ciphermysteries.com/.

129. G.W.L.Hodgins, "2011 Forensic Investigation of the Voynich Manuscript," presented at the Voynich 100 Conference, Frascati, Italy, May 2011. Also reported on in A.J.T.Jull, "Some Inter-esting and Exotic Applications of Carbon-14 Dating by Accelerator Mass Spectrometry," 10th International Conference on Clustering Aspects of Nuclear Structure and Dynamics, Journal of Physics: Conference Series 436 (2013): 012083.

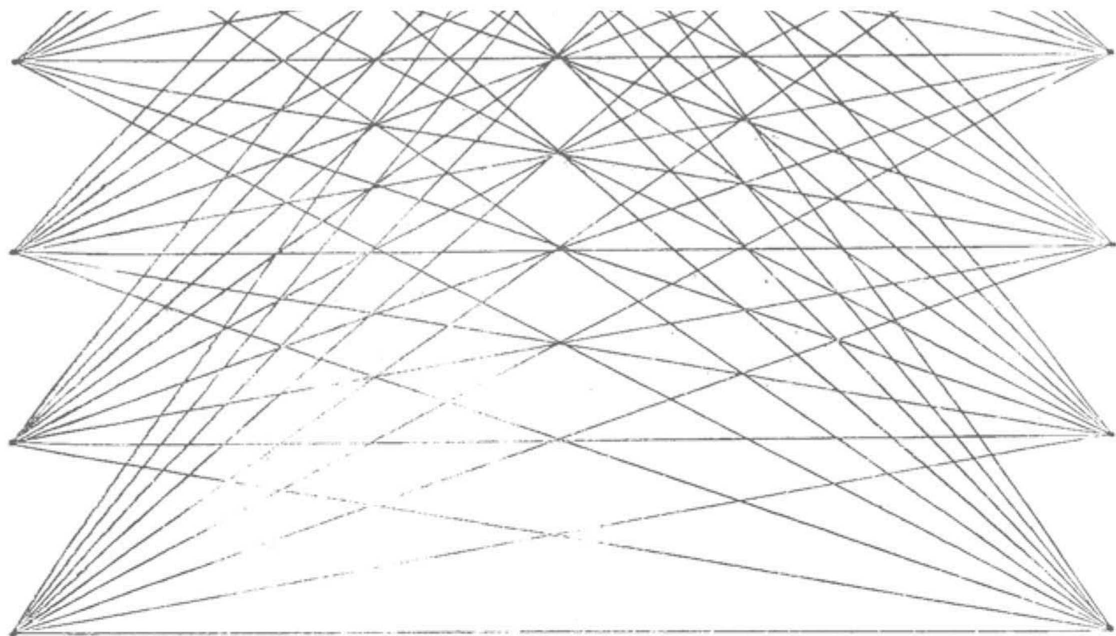
130. Sravana Reddy and Kevin Knight, "What We Know about the Voynich Manuscript," Proceedings of the 5th ACL-HLT Workshop on Language Technology for Cultural Heritage, Social Sciences, and Humanities, Portland, OR (June 24, 2011), (Madison, WI: Omnipress, Inc.),

78–86.

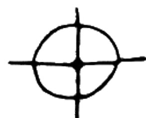
131. David Kahn, The Codebreakers (New York: Macmillan, 1967), 863.



第2章
古董上的密码



在文字之外



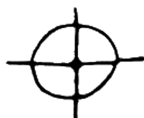
根据碳–14测年法的鉴定结果，我们已经确认伏尼契手稿所使用的皮纸制造于15世纪。虽然伏尼契手稿已经有超过500年的历史了，但它还称不上世界上最古老的未解之谜。

几乎每一个发明了文字的文化都在之后不久就进一步产生了秘密书写的技术。虽然在每一种拥有文字的文化中都存在一些被公认是密码的例子，但是事实上，还有一些其他神秘的信息，专家们却拒绝认定它们为密码。这些信息看起来像是一些随机的符号和字母，于是专家们认定，它们一定是不识字的人试图模仿文字而创造出来的，毫无意义，它们通常被称为“无意义文字”。

我们知道，从表面上来看，密码就像是一串随机的字母，而不识字的人所写的无意义文字看起来也像是一串随机的字母。那么，专家们是如何区别密码和无意义文字的呢？事实上，很多研究者都没有考虑过密码和无意义文字之间的微妙区别，而是随意地下了结论。这些研究者并非密码专家，他们甚至根本没有考虑过这些奇异的文字也许是密码这种可能性。我们应该高度关注的一项事实是，在很多情况下，这些我们看不懂的文字并不是随手乱涂乱画的，而是精心创造出来的艺术作品。有时，这些文字被刻在石头上，有时，它们出现在非常严肃的宗教背景中。这其中有很多例子，其中包括维京人的如尼文符文石（runestone，维京人在密码学方面的知识与古希腊人不相上下），古希腊绘有图案的花瓶，以及古埃及的石棺。

在本章中，我将向读者详细介绍几种极少有人能理解的文字，并展现一些有趣的插图。到目前为止，似乎尚未有人以跨文化的视角对无意义文字进行过概括和总结，而本章的内容也许是这方面的首次尝试。

语言和密码



我们需要知道，口语和书面文字是两个不同的概念。在某些语言中，同样的语言可以用不同的文字进行书面表达，比如日语。在日语中有汉字、平假名、片假名、罗马字（用拉丁字母来表达日语的书写方式）等不同的写法。因此，在日语中，“书”可以写作“本”（汉字）、“ほん”（平假名）、“ブック”（片假名），或者“hon”（罗马拼音）。除了片假名“ブック”之外，其他三个词虽然写法不同，但是它们的读音是完全一样的。

同样，同一种文字也可以用来表示多种不同的语言。英语字母和德语字母几乎是完全一样的（英语字母和德语字母都被归为拉丁字母），然而它们却代表着两种不同的语言。

由于上述两种现象的存在，导致即使我们看到了某种文字，有时候也不能明确无误地判断出这些文字代表的究竟是何种语言。如果我们发现了一段古代文字，这些文字既不能与任何我们已知的语言相匹配，又没有办法读懂，我们就必须考虑以下几种可能性：

1. 这可能是在用一种我们熟悉的文字来表示某种语言，但是此前尚没有把这种语言和这种文字联系起来的先例。

2. 这些文字可能代表一种失传已久的语言。

3. 这段文字可能是对某种已知或未知的语言加密后得到的。

不管这段古代文字究竟属于以上哪种情况，我们都可以使用密码学的工具来解决这个问题。要破译这类古代文字背后的意义，我们所用到

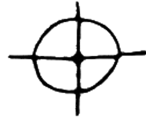
的技巧与密码分析的技巧有许多共通之处，无论这些古代文字有没有经过加密处理。但是，有时候，我们很难判断一段文字究竟属于上述三种情况中的哪一种。在历史上，曾经有过这样的先例：有时，一段表示自然语言的文字会被错误地判断为一段加密文字。

约瑟夫·阿莱维（Joseph Halévy）是用科学方法研究语言的先驱。1873年，阿莱维提出，苏美尔语不过是一种僧侣使用的秘密书写方式，并不是一种口头语言。这场争论一直持续到了1900年，最终，证据显示阿莱维的观点是错误的。

虽然在上面的例子中，所谓的“秘密文字”事实上是一种正常的文字，但是在发现并成功破译了很多苏美尔语文稿之后，人们得出结论，苏美尔语中确实存在一种原始的密码形式。比如，有些时候，神的名字会被密码数字所取代。在文献中，这种现象被称为“Götterzahlen”（德语，意为“上帝的数字”）。总的来说，在各种文化中，密码的发明常常紧跟着文字的发明。当识字的人很少时，文本本身就像是一种密码。然而，随着识字人口的增多，如果我们想把某些秘密隐藏起来，不让其他识字的人知道这些秘密的话，秘密书写的技术就显得非常必要了。此外，宗教文献也常常会用到密码。即使在今天，仍有一些人从来不会写出“上帝”（God）这个词——因为任何写有这个词的纸张都可能被毁坏，这就是在亵渎神明。当这些人需要使用“上帝”一词时，他们会写下“G–d”作为替代。这样，即使写着这个词的纸张被毁坏，也不会对上帝不敬。

接下来，我将举几个来自不同古代文明的例子。我认为它们有可能是一些尚未破译的密码。研究这些古代文明的专家通常认为这些例子只是无意义的胡言乱语，即“无意义文字”。然而，我们知道，过去曾有专家把有意义的正常文字误判为“秘密文字”的例子，因此，今天的专家也完全有可能把密码文字误判为“无意义文字”。

古埃及石棺的秘密



在我们已知的古文明中，苏美尔语背后的文明是历史最悠久的一种。当然，某些古代遗址，比如位于今天土耳其境内的哥贝克力石阵（Göbekli Tepe）显示，人类文明还可以追溯到更久远的过去。然而，由于我们在这些遗址中没有发现文字记录，我们对这些文明的了解微乎其微。古埃及文明出现的时间比上述这些古文明稍晚一些，对于19世纪早期的人们来说，古埃及人的文字就像苏美尔语一样，是一些完全无法读懂的神秘符号。破译古埃及象形文字的故事非常有趣，但是，现在我们要讨论的是另外一种至今尚未破解的古埃及密码。

第一个例子是一个有争议的石棺。这个石棺保存于斯旺西大学的埃及中心惠康博物馆。这个石棺上的绘画风格与古埃及第26王朝的风格相匹配，第26王朝大约存在于公元前600年左右。然而，这个石棺的长度只有20英寸多一点儿，并且我们对它上面的象形文字完全无法做出有意义的解释。这个石棺会不会是近代人为了满足学者和收藏家的需求而仿制出来的一件赝品呢？显然，当古埃及人为了神圣的葬礼制造这样一副石棺的时候，他们是不会在石棺表面写上无意义的象形文字的。为了搞清楚这个问题，最直



接的调查方法是研究这个石棺的来源。不幸的是，该博物馆并不知道亨利·所罗门·惠康爵士（Henry Solomon Wellcome，1853—1936）究竟是以何种方式、在何地获得这件藏品的（这个石棺的藏品号码为W1013）。博物馆只知道这件藏品是于1971年进入该馆的。

有些人认为，这个石棺是一件制造于现代的赝品。然而2014年，斯旺西大学医学临床影像学院的保拉·格里菲思（Paula Griffiths）对这个石棺进行了CT（计算机断层成像）扫描，扫描结果并不支持这种论点。现代CT扫描技术显示，这个石棺中有一个带胎盘囊的胎儿。这个胎儿只有约3英寸长。埃及中心的馆长格雷夫斯–布朗估计，这个胎儿大约有12~16周大。石棺中的大部分空间被其他东西塞满，据判断这些东西是折叠后的麻制绷带。此外，这次CT扫描还发现，石棺中还有可能是护身符以及珠串、流苏之类的物品，这些都与第26王朝的葬礼风俗相吻合。

虽然我们很难想象有人会用一个真实的人类胚胎来仿制假古董，然而文献中确实记载过此类的变态行为。在一本关于假艺术品的书

图2-1 一个有争议的石棺。它究竟是来自古代还是现代？

中，有这样一段话：

> 1485年，罗马的亚壁古道——对于一位文艺复兴时期的古典文学专家而言，这里简直就是一台帮你找到珍稀古董的时光机——上发现了一座古墓，古墓里有一具保存极为完好的年轻貌美的女孩的尸体。石棺上的拉丁文显示，这位女性正是图莉奥拉（Tulliola）。图莉奥拉是西塞罗美丽的独生女，她芳年早逝。石棺上刻着西塞罗令人落泪的凄美文字："献给图莉奥拉，他唯一的女儿。除了早逝，她从没有犯过任何过失。（Quae nunquam peccavit nisi quod mortua fuit.）这个纪念碑由她悲痛的父亲西塞罗所立。"
>
> 发现图莉奥拉的石棺引起了轰动，而且没有任何人对此事提出质疑，就连最爱怀疑的批评家也接受了这一发现。然而，事实上石棺上引用的这句话并不是西塞罗的话，而是来自另一个可靠的古代拉丁文来源。但是，似乎没有任何人在意这个疑点。在此后不久，罗马各地又发现了若干处所谓的"图莉奥拉墓"。接着，在佛罗伦萨和马耳他也同样发现了所谓的"图莉奥拉墓"，每一处墓中都有一具保存完好的年轻女性的尸体。安东尼·格拉夫顿（Anthony Grafton）写道："在接下来的100年中，'图莉奥拉的坟墓'成为深受游人喜爱的观光胜地。"然而，这些年轻的女孩究竟是谁，她们是怎样死去的，她们究竟因何而死，这些问题光是想一想就已使人毛骨悚然了。然而，人们一直都没有确认这个可怕的骗局的始作俑者究竟是谁。(注)

虽然古埃及石棺上的文字意义不明，虽然我们在上文中提出了这种可怕的可能性，但是新的证据使专家们终于确定，那个古埃及石棺确实是一件真品。

下面，让我们来考虑一些极端的情况。假如每一副古埃及石棺上都刻有一些无法解读的文字，那么我们显然有理由相信，这些文字对古埃

及人而言是有意义的，只是我们尚未破译出来而已。但还有一种情况是，如果只有一个古埃及石棺上有我们无法看懂的标记，那么这些“文字”很可能是因为某种形式的错误而产生的，这使我们确实无法做任何有意义的解读。那么，除了这两种极端情况之外的情况又应该怎么处理呢？到底需要有多少个这样的例子才能让世人相信，石棺上这些看似无意义的文字其实是有意义的呢？

事实上，文献记载的刻有无意义文字的古埃及石棺远不止上面这一个！在萨卡拉发现的来自第21王朝的石棺上，也有多种意义不明的文字，这些文字有时被称为“假象形文字符号”。官方的解释是：这些符号能够“在死者死后的生活中为他们提供魔法的帮助”。(注)

现在，我们已经有了来自第21王朝和第26王朝的例子，这些例子是否已经足够了呢？在这两个王朝之间的其他王朝中，有没有这样的例子呢？关于这一话题，弗林德斯·皮特里（Flinders Petrie）爵士曾有过如下讨论：

> 对于伊拉胡恩金字塔而言，下一个重要时期是第22王朝到第25王朝。金字塔附近的山丘已有很大一部分被用于修建石室坟墓以及金字塔时期的马斯塔巴(注)，但它们在很早时就已经遭到偷盗和破坏，被破坏后的遗址在较晚的布巴斯提斯王朝和埃塞俄比亚王朝中又被再次使用。这些葬品通常都比较粗糙，棺材上很少有能被解读的文字，大部分都是由不识字的棺材装饰师画上去的常规图案。(注)

也就是说，在上述这些王朝中，在棺材上写上无法辨认的文字事实上是一种常规的行为！把完全无意义的文字写到深爱之人的棺材上，这种风俗是否有可能存续超过6个王朝的时间呢？由于皮特里爵士认为这些文字只是一些有错误的假文字，因此他并没有花太多时间来研究它们。皮特里爵士还在另外一段文字中提到这些无意义的文字，现在我将这段文字摘录于下，并且为读者标注出一些需要强调的部分：

作为总结，接下来我将介绍第22王朝的一些典型的葬礼细节。棺材通常较薄，侧面倾斜，肩部微微凸出，头部为圆形。棺材盖有棱边，中部刻有文字，这些文字通常是无意义的文字，尾部会省略人名。头部和肩部有浮雕，有时手部也有浮雕。脸部通常是一块雕刻过的木头，头部装饰有时是用灰泥做成的，更常见的是用尼罗河的泥做成的。棺材用红、蓝、黄、黑以及白色等鲜艳的颜料粉刷，配以用假发以及秃鹫毛做成的头饰。棺材内用麻制品或者石膏制品放置木乃伊，它们按尸体的形状塑形，背面可以分开，这样就可以把木乃伊从背面塞进去。这个装置表面通常是白色的，中间有一列文字。上方是一个展翅的秃鹫，有时还有一个羊头。脸被刻在木头上，然后插入棺材中（因为放木乃伊的装置会腐烂或破碎，所以有时会出现多重脸的图案），头部画上假发。有时候，放置木乃伊的装置上也会画满祭神的场景。棺材中的木乃伊很少有护身符，且早已变成了黑色的灰烬或骨头。(注)

纽约皇后学院的艾伦·R.舒尔曼（Alan R.Schulman）谦虚地提出了一种比较少见的观点。以下文字引自他的一篇论文，这篇论文讨论的是在古埃及的一块甲虫形宝石上发现的一段奇怪的文字，但作者似乎认为，以下这种观点完全可以被推广到更宽泛的情景中去。舒尔曼写道：

然而，文字应该包含某种意义。毕竟，古埃及人是有逻辑的，他们不会把无意义的胡言乱语刻下来。如果我们看不懂一段文字，最有可能的解释是：我们还没有破译这段文字的意义。我们不应该因此认为这段文字本身就是没有意义的。(注)

然而，在破译这些文字背后的意义之前，我们必须先对古埃及人的密码学知识有更深入的了解。在古代埃及，密码学究竟有多长的历史？古埃及人使用过什么样的加密技巧？约翰·科尔曼·达内尔（John Coleman Darnell）是耶鲁大学的埃及学助理教授，他曾以自己在芝加哥

大学完成的博士论文为基础，出版过一本这方面的书。在这本书中，达内尔写道：

> 密码最早出现于古王国时期，并在第一中间期以及中王国时期继续流传。在新王国时期，密码已大量存在，在王室头衔中，在私人墓穴的铭文中，在一些个人的涂鸦中，以及在王室坟墓中保存下来的各种冥府书籍中，都可以看到密码的身影。在古埃及后期、整个托勒密王国时期，以及罗马时期，密码达到了复杂的高峰，埃斯纳神庙的文字就是证明。一些此前只存在于加密文字中的符号以及符号价值此时已经广泛出现在各种象形文字中。[注]

也就是说，从古王国时期一直到象形文字终结时，古代埃及人一直都在使用密码！在接下来的若干个世纪中，某些曾经被视作密码的文字已经变得非常主流，因而变成了一种正常的书写形式。下面这个例子可以让读者更加清楚地理解这一点。

古埃及人曾经使用一种替代密码，在这种替代密码中，人们把某个象形文字用与其主题意思类似的另一个象形文字代替。比如，象形文字“”可以用象形文字“”来代替。此后这个符号又可以被“”代替。以上三个符号都表示“嘴巴”。第一个符号代表从正面看的嘴巴，第二个符号代表的是从侧面看的嘴巴，而第三个符号代表的是鳄鱼的嘴巴。

在另外一些例子中，古代埃及人会用与某个象形文字形状类似的其他象形文字来代替它。比如用“”来替代“”，或者用“”来替代“”。

除了上面两种替代方式以外，还可以用与某个象形文字读音类似，但形状不类似的其他象形文字来替代它。

上面这些替代方法都在不断升级，因为随着这些替代方法变得越来越常用，了解这种替换方法的人也越来越多，所以，想把自己的文字加

密的人就不得不发明出新的替代方式。随着这一过程的演化，古埃及的密码变得越来越复杂难解。这就是为什么一般来说，越古老的埃及密码越容易破译，而晚期的埃及密码则更加难以破译。

除了上面这些替代型加密方式以外，古代埃及人还会使用一些与上述技巧截然不同的加密方式。在这种加密方式下，象形文字符号本身不变，但是它们排列的顺序改变了。数学家和计算机科学家将这种加密方式称作“换位重排”，而埃及学家则称之为“扰动”。

艾蒂安·德里奥东（Étienne Drioton）曾在古埃及密码的破译方面做出过突破性的工作。他在论文中提到，这种加密方式最常被用于甲虫形宝石上的文字。他还举了一个小例子：假设我们有如此排列的4个象形文字“”。德里奥东用扰动（重排）后的顺序来读这4个字，读取的顺序就变为“1 3 4 2”。于是我们就得到了“”，意思是“孔苏会保护（我）”。[注]虽然德里奥东指出这种换位重排后的文字一般都相当简短，但是他也举出了一个例外的情况。在巴黎的吉美博物馆中，有一个古埃及的杯子，上面有一段包含21个符号的文字，就是用上述这种换位重排的方式书写的。[注]

此外，还有更加华丽的例子。在图坦卡蒙的第二座黄金神龛上，就用到了这种换位重排的方法。这种换位重排的方式还在其他许多地方出现过。

达内尔指出，目前我们对古埃及密码的认识还非常不足，他写道：

> 对于古埃及后期之前的所有密码，我们还没有系统地研究过。这方面的研究结果与古埃及后期密码研究结果相比较，会给我们带来许多新的认识。但目前，针对古埃及后期密码的研究同样没有起步。[注]

虽然少数人在这方面做出了努力和探索，但是目前这方面的研究仍

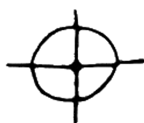
然是空白，公众对这一领域的看法是造成上述现象的重要原因。艾伦·R.舒尔曼写道：

> 埃及学家早就知道，古埃及人经常使用各种形式的密码来书写某些铭文。但是由于某种原因（可能由于这个问题过于复杂），大部分学者选择不对这些密码进行深入的研究。但是，这方面也有一个非常突出的特例：已故的艾蒂安·德里奥东在古埃及密码的研究领域取得了十分优秀的成果，尤其对甲虫形宝石上的密码颇有建树。他的工作为未来所有对古埃及密码的调查和研究打下了坚实的基础。注

也许，在不久的将来，会有学者开展上述这些领域的研究。到那时，我们将对那些我们现在认为毫无意义的文字有更深的理解。上文中提到的那个小小的石棺上的文字究竟会告诉我们怎样的故事呢？

古埃及人留下的可能的密码远不止石棺上的铭文这一种。参考文献和延伸阅读部分可以帮助有兴趣的读者进一步了解这方面的内容。

古希腊花瓶上的密码



接下来我要向读者介绍另一种文明的密码——古希腊密码。我们对古希腊密码的了解比对古埃及密码的了解要多一些。事实上，“密码”（cryptography）就来自希腊语的“κρυπτός（kryptos）”和“γραφία（graphia）”，这两个希腊语单词的意思分别是“隐藏”和“书写”。

我们知道，古希腊人会使用单套字母替代式密码（前面所介绍过的MASC密码），即把明文的每一个字母都用其他字母替代。但是除了MASC密码以外，古希腊人还掌握了一种把字母转化成数字的加密方式，叫作“波利比奥斯密码”（Polybius cipher）。它使用一种长方形的棋盘状字母表进行加密。如果用英文字母来举例的话，这种字母表如下：

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

而希腊语版字母表如下：

	1	2	3	4	5
1	α	ζ	λ	π	φ
2	β	η	μ	ρ	χ
3	γ	θ	ν	σ	ψ
4	δ	ι	ξ	τ	ω
5	ε	κ	ο	υ	

不管字母是以横排、竖排还是随机的顺序放进网格中，都不会影响这一系统的工作方式。在发明这个系统的时候，发明者已经考虑到了远距离信号传输方面的应用。在《历史》（*Histories*）一书中，波利比奥斯解释了这种加密系统的工作原理，并且把这一系统的发明归功于克莱奥塞诺斯（Cleoxenus）和德谟克利特（Democritus）。

在波利比奥斯给出的例子中，发送信号的人希望发出一条信息，开头几个字母是κ，ρ等，为了表达κ这个字母，发送人左手拿2个火把（表示第2横行），右手拿5个火把（表示第5竖列）。发送人要留给收信人足够长的时间，保证后者能看清他手中的火把数目。然后，发送人改为左手拿4个火把，右手拿2个火把，以表示字母ρ。在现代的书籍中，一般都把这种字母表写成上面的方形棋盘状的形式。但是，波利比奥斯却以一种稍微不同的方式来呈现这种棋盘字母表。对古希腊人而言，每一个竖列都是一个单独的字母表，因此发送人和收信人面前各自会摆上5份字母表。发送人左手所持的火把数目代表此时应该看第几份字母表。

把所有希腊字母放进一个5×5的网格中以后，还有空余的地方，而5×5的网格却不够放入所有的英文字母。为了解决这个问题，字母J被去除了（或者可以认为字母J与字母I合并为同一个字母）。我们可以用这个网格来写出一段书面密码，只要把每个字母用这个字母所在的横行数和纵列数代替就行了。比如，柏拉图的名言“Only the dead have seen the end of the war（只有死者才能看到战争的终结）”，经过加密处理后就变成了以下这个句子：

```
O  N  L  Y  T  H  E  D  E  A  D  H  A  V  E  S  E  E
34 33 31 54 44 23 15 14 15 11 14 23 11 51 15 43 15 15

N  T  H  E  E  N  D  O  F  T  H  E  W  A  R
33 44 23 15 15 33 14 34 21 44 23 15 52 11 42
```

看完以上这个例子后，有些读者可能会认为，完全由字母构成的密码不可能是波利比奥斯密码，但事实并不是这样。我们也完全可以用字母表示棋盘字母表的横行和纵列。

	A	D	F	G	X
A	A	B	C	D	E
D	F	G	H	I	K
F	L	M	N	O	P
G	Q	R	S	T	U
X	V	W	X	Y	Z

事实上，这就是第一次世界大战期间德国曾经使用过的一种加密系统的第一步，只不过网格中的字母顺序被打乱了。德国人选择A、D、F、G、X这5个字母作为密码字母，因为在以莫尔斯电码发送信息的时候，这5个字母不容易混淆。之后，德国人进一步扩展了上述字母表，增添了加密后的数字，这样就不需要用单词的形式把数字拼写出来了。为了加入数字，他们在上述字母以外又添加了新的行和列，并被标记为V。

因此，即使是完全由字母构成的密码也有可能是波利比奥斯密码。但是，只有在字母总数比较小的时候，才能使用这种加密方法。

普卢塔克（Plutarch）在他所著的《来山得的生平》（*Life of Lysander*）一书中描述了斯巴达人使用的一种加密方法，这种加密方法与上述的波利比奥斯密码截然不同。这本书描写的是公元前5世纪的一位斯巴达上将的生平。我把该书中的相关段落摘抄如下：

> 当五长官[注]派某人担任军队的将军或者上将的时候，他们会事先准备两根圆形的木棍。这两根木棍的长短和粗细完全一致，头尾互相吻合。五长官持有其中一根木棍，另外一根则交给被派遣的将领。这样的木棍被称为斯基塔里密码棒（skytale）。当五长官需要把某个非常重要的机密信息传达给外派将领时，他们会将一张狭长的纸条缠在这个密码棒上，让纸条不留任何空隙地完全覆盖住整个

密码棒，之后，再在这张包裹在密码棒上的纸条上书写。写完信息以后，五长官会把这张纸从密码棒上揭下来传递给外派的将领。当外派的将领收到这个信息时，它是完全无法被读懂的，因为纸张上的字母之间看似没有任何联系。但是，只要将这张纸条缠到他所拥有的那根密码棒上，纸条原本不相邻的地方就会匹配起来，于是外派将领就能够读出五长官发来的整条信息了。这张纸条也和木棒一样被称为斯基塔里，因为被度量的东西可以用度量物的名字来命名。[注]

斯基塔里密码棒［skytale，读音与“Italy”（意大利）押韵］是目前已知最古老的通过换位重排法来加密的工具。有人怀疑，指挥官的权杖就是从斯巴达人的斯基塔里密码棒演化来的。



图2-2 用斯基塔里密码棒写成的一条信息

尤利乌斯·恺撒把希腊字母表当作密码字母表来使用。有时，他只

是很简单地把拉丁字母替换成相对应的希腊字母。比如，将明文“GOLD”替换以后对应的密文就是“ΓΟΛΔ”。然而，在这方面古希腊人却并没有做到“礼尚往来”，古希腊人很少使用外来的字母表来对信息进行加密。

当然，我们对于希腊密码的总结肯定不够完整。到目前为止，学者已经理解的这部分希腊密码也许只是冰山一角。我们不妨考虑一下古代戏剧的情况。根据历史记载，索福克勒斯一共创作了123部戏剧，但其中只有7部被完整地保存下来。其他古代著作保存下来的概率也同样非常低。而且，以上我们谈到的还仅仅是一些广为流传的作品。记载着密码这种保密艺术的书卷保存下来的概率肯定更低！但是，我们今天还能看到一些蛛丝马迹，从中我们可以猜到那些已经失散的书卷中究竟包含怎样的内容。

艾伯特·C.莱顿（Albert C.Leighton）对破解历史密码有着特殊的兴趣。莱顿注意到，在奥卢斯·格利乌斯（Aulus Gellius）写于公元2世纪的著作《阿提卡之夜》（*Attic Nights*）中，作者含糊地表示了当时存在比目前已知的任何古代世界的密码都更复杂的密码。此外，莱顿还引用了一封公元4世纪的信，在这封信中，奥索尼乌斯（Ausonius）声称，他知道“古人用来隐藏和破译秘密信息的大量密码”。[注]莱顿据此猜测道：“有可能古代的密码比文献中显示的要更加高级，并且它们还影响了文艺复兴时期的密码。”[注]

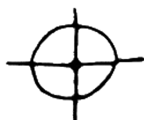
接下来，我很快就会谈到一些出现在古希腊花瓶上的奇怪文字。通过陶器上的文字来研究古希腊文字是一种非常自然的选择，因为现存最早的古希腊文字（来自公元前8世纪中期）就是在陶器上发现的。此外，阿提卡花瓶（即来自雅典的花瓶）上保存下来的文字不仅制作日期很确定，而且是所有文字种类中数量最大的一类。而且，包含文字的这类文物的数量还在不断增加，因为目前仍有大量花瓶及其碎片不断被挖掘出土。

这些文字有时应该从左向右读，有时应该从右向左读，但是从左向

右读的情况更加常见一些。因此，当我们发现一段可能是密码的文字时，我们需要考虑从不同方向阅读这段文字的可能性。

下文将要讨论的许多花瓶都来自雅典，因为和古希腊其他城邦的艺术家相比，雅典的艺术家更喜欢在花瓶上添加文字。如果你不识字而想假装识字，那么雅典可不是一个好地方，因为雅典是古希腊的文化中心和知识中心。[注]然而，许多研究雅典花瓶的专家却认为，从公元前25年开始，雅典的花瓶上开始出现一些“无意义的文字”。这些无意义的文字有时只是一个单词，有时则是一串单词。虽然科林斯花瓶上也出现过一些这类无意义的文字，但是专家相信这种现象最先出现于雅典，因为带有无意义文字的雅典花瓶数目远超过科林斯花瓶的数目。在这个时间段中，识字的希腊人正在上升。我们在前文中已经提到，当识字的人很少时，书写本身就起到了密码的作用。然而，一旦识字的人提高，就需要用一些更加复杂的方法来对信息进行加密。因此，识字人口上升的时段正是最容易出现密码的时段。

被加密的签名



当我得知古希腊花瓶上存在这类无意义的文字时，我脑海中产生的第一个想法是：这些无意义的文字可能代表着加密的签名。也许制造这些花瓶的艺术家由于某种原因不能在花瓶上署名，但他们可以用加密的方式绕过这些规则，把自己的名字写在作品上。于是，我对此进行了深入的研究。我很快就发现，古希腊的工匠们是可以在花瓶上署名的，但是在很多花瓶上却并没有出现作者的名字。有些花瓶上会出现两个署名，一个是雕塑者/制陶者的名字，另一个是画家的名字。

制陶者的名字后面跟着希腊语中的“ἐποίεσεν（*epoiesen*）”（意思是“制造了它”）一词。但是，即使后面有这个词，这个签名仍有可能不属于制陶者，而属于工坊所有人或者设计者。而画家的名字后面跟着希腊语中的“ἔγραπσεν κἀποίεσεν”（意思是“绘制了它”）。奇怪的是，有些花瓶上出现了“ἐποίεσεν（*epoiesen*）”，但却没有与之相连的签名。当一个花瓶上既有制陶者的名字又有画家的名字时，制陶者的名字会出现在画家名字的前面。

有时候，花瓶的制作者和绘画者是同一个人。在这种情况下，如果花瓶上有这位艺术家的署名的话，后面会跟着希腊语中的“ἔγραπσεν κἀποίεσεν”（意思是“制造并绘制了它”）。

艺术家虽然会在一些作品上署名，但是他们并不会对所有作品系统性地署名，署名的那部分作品也并不一定是该艺术家最优秀的作品。通过风格对比，我们可以鉴定出大约900位古希腊花瓶艺术家，但我们只知道其中大约40位艺术家的名字。为了方便地指代其他无名的艺术家，研究古希腊花瓶的学者会给这些艺术家取一些假名作为代号。

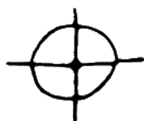
此外，研究者还发现了一些虚假的署名。虽然包含这些署名的花瓶本身是真品，但是古代的艺术家在花瓶上署上了假名。而不管花瓶上的署名是真是假，包含署名的花瓶只占所有花瓶总数的不到1%。

根据上述情况我们可以基本确定：即使在某些花瓶上出现了加密署名，加密本身也并不是必需的。虽然这些署名并不符合姓名首字母缩写的规律，但是艺术家仍有可能出于某种原因而选择在花瓶上留下加密署名。测试上述假说是否属实的方法之一是研究这些无意义文字中的字母是否具有某种规律。这些字母的规律是否匹配某位已知艺术家的姓名，或是该时期任一常见的希腊名字呢？如果猜测出了艺术家的名字，我们还需要比较这件艺术品的风格是否与该艺术家的风格相符，或者这件花瓶的艺术风格是否与其他带有相同无意义文字的花瓶相一致。

一种比较流行的观点认为：不识字的艺术家故意将这些无意义的文字写到花瓶上，目的是为了让可能有意购买花瓶的人觉得这些作品更有

吸引力。然而，这种做法同时也会限制这些作品的潜在市场范围。任何一位识字的顾客可能都不屑于购买这些写有假文字的艺术品。而且，如果一个不识字的顾客购买了这种花瓶，那么当他的某位识字的朋友告诉他花瓶上所写的字毫无意义时，他会有什么样的想法呢？显然，这位顾客再也不会从同一个卖家那里购买其他花瓶了。因此，在花瓶上写上无意义的文字似乎并不是一种十分明智的市场营销策略。

一种新的方法



我们发现，同一位艺术家有时在花瓶上留下有意义的文字，有时却留下无意义的文字。此外，我们还发现，有时在同一个花瓶上既有有意义的文字，又有无意义的文字。事实上，这种情况不仅局限于花瓶这一类物品。收藏于法国卢浮宫的《怜子门农图》（约公元前490—前480年）上就同时出现了有意义的文字和无意义的文字。

门农为了捍卫特洛伊而死，但是门农的命运在上述这个悲惨的情景发生以后经历了转机。厄俄斯的眼泪感动了宙斯，于是宙斯决定让门农获得永生。《怜子门农图》右侧的文字提到了门农的名字，并且还留下了这个盘子的制造者和画家的名字。然而，它左侧的文字却比右侧的文字更加有趣。

最后两行文字“HERMOΓENES KALOS”可以翻译为“埃莫根尼（Hermogenes）是美丽的”。但是，最上面的“EENEMEKNERINE.”似乎是一行无意义的文字。

为什么艺术品上会同时出现有意义和无意义的文字呢？对此，专家

提出了一系列解释，但是这些解释都不是很有说服力。1957—1977年期间北卡罗来纳大学希腊学教授亨利·R.伊默瓦尔（Henry R.Immerwahr）这样写道：

> 有些花瓶上既有有意义的文字，也有无意义的文字，且这两种文字是由同一位画家写到花瓶上去的。我们由此可以清楚地推断，在大部分情况下，这些无意义的文字是由识字的艺术家故意写上去的。由于某种原因，这些艺术家认为作品上应该留有文字，但却并不想要通过这些文字传递某种精确的信息。(注)

作者究竟是如何“清楚地推断”出以上这种结论的？对我来说，上述说法成立的可能性是非常低的。艺术家是一些非常具有创造力的人。我很难想象这些富有创造力的人会经常不知道该往作品上题写什么内容，于是只能胡乱写一通。根据伊默瓦尔的理论，艺术家有时会这样做：他们觉得作品上的题词还应该更长一些，但是实在不知道该写些什么，因此决定写上ehujf ki fengoku wfscph！

读者能看出这种理论有多么傻了吧？

关于这一点，约翰·博德曼（John Boardman）爵士做出了以下论断：

> 在有些例子中，有意义和无意义的文字紧挨着出现，这种情况说明，这些文字结合了从别处抄来的文字和匠人自己的想象。(注)

按照博德曼爵士的说法，一位不识字的艺术家小心地从别处抄来了一段有意义的文字，然后却在同一件作品上写上了自己随意创造的胡言乱语，从而成功毁掉了识字的顾客购买这件作品的可能性。

当然，也有另外一些研究者认为，这些花瓶上的所谓“无意义文

字”实际上是具有某种意义的。对于这些研究者而言，同时出现有意义和无意义的文字的作品无疑是最值得深入研究的。斯坦福大学古典学系的阿德里安娜·梅厄（Adrienne Mayor）就进行了这方面的研究。她研究了一系列来自古希腊的花瓶，这些花瓶上都出现了亚马孙女战士或塞西亚人（Scythian）的图像，并且都同时包含了有意义和无意义的文字。

梅厄说：“一开始，我只有一个模糊的直觉。我想：这些描绘亚马孙女战士和塞西亚人的古希腊花瓶上的无意义文字会不会实际上具有某种意义呢？”注

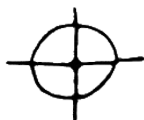


图2-3 阿德里安娜•梅厄

梅厄认为，这些文字也许是根据读音用希腊字母拼写出来的外国名字。它们所以在希腊语中看起来毫无意义，是因为它们代表的并不是希腊语的名字。

为了验证上述假说，梅厄和另一位研究希腊花瓶绘画和肖像的专家戴维·桑德斯（David Saunders）一起，挑选出了几个符合她的标准的古希腊花瓶，并将这些花瓶上的无意义文字部分（尽量剔除上下文）呈送给了一位比较历史语言学家——约翰·科拉鲁索（John Colarusso）。科拉鲁索的专业领域包括西北高加索语（切尔克斯语、阿布哈西亚语、尤比克语）、奥塞特语、古格鲁吉亚语、古希腊语、伊朗语，以及其他一些语言。因此，如果花瓶上的这些文字确实有意义的话，科拉鲁索有很大概率能够辨别出这些写在希腊花瓶上的外国文字是用何种语言写成的。

拿外国人取笑？



但是，我们还应该考虑到这样一种情况：这些花瓶上的文字可能只是希腊人写下来嘲笑外国人的。我们知道，古希腊人是有这种先例的。对于希腊人来说，某些外国语言听起来就像一些无意义的音节，比如bar-bar-bar-bar，于是希腊人会把说这些外国语言的人称为“βάρβαρος（barbaros）”。事实上，英文中的“野蛮人”（barbarian）一词就是从这个希腊语单词发展而来的。

事实上，在现代社会中，也存在这种玩笑的例子。翁贝托·埃科（Umberto Eco）的小说《傅科摆》（*Foucault’s Pendulum*）中就有这样的情节：一个名为阿布（Abu）的电脑程序创造出了一段虚假的外语文字。

转换前的原文：

Abu, do another thing now: Belbo orders Abu to change all words, make each “a” become “akka” and each “o” become “ulla”, for a paragraph to look almost Finnish.

（阿布，现在做另一件事情吧。贝尔勃让阿布把这段文字中所有的“a”改成“akka”，所有“o”改成“ulla”，这样就产生了一段看起来很像芬兰语的文字。）

Akkabu, dulla akkanullather thing nullaw: Belbulla ullarders Akkabu tulla chakkange akkall wullards, makkake eakkach “akka” becullame “akkakk-akka” akkand eakkach “ulla” becullame “ullakka,” fullar akka pakkarakka-grakkaph tulla lullaullak akkalmullast Finnish. 注

埃科是一名符号学的教授，因此，他可能是真实世界中最接近小说家丹·布朗塑造的男主角罗伯特·兰登的人了。

在这些古希腊花瓶上的无意义的文字中，出现过一些奇怪的例子，比如在同一个词中会出现4次“kh”的字母组合。这种情况看起来确实像是在用一种夸张的方式来模仿外国人的语言或者口音。或者，也有可能是花瓶的绘制者认识某位说话结巴的人，并且拥有一种爱德华·埃尔加（Edward Elgar）式的幽默感（我们将在本书第3章中谈到爱德华·埃尔加）。古希腊人用字母X（chi）来表示“kh”这个音，在某些希腊喜剧中，确实有重复使用这个音节来嘲笑塞西亚人的例子。

另外一种可能性是：这些看似无意义的文字实际上表示的是音效。对于一个不以这种语言为母语的人来说，由于不熟悉这样的传统，这些表示音效的文字看起来就像是无意义的文字。电视剧《生活大爆炸》（*The Big Bang Theory*）的第4季第9集曾经谈到这个问题。在该集的故事中，谢尔顿问拉杰什：

> 你确定你已经准备了足够多的漫画书吗？要知道接下来你要花12个小时监控望远镜，而根据我的估计，你带的漫画书只够读7个小时。而且，我的这种估计已经考虑到了你在理解漫画书中的“Bamf”“Snikt”等词时会遇到的困难(注)。(注)

古希腊花瓶上的这些文字可能没有什么深刻的含义，只是用来取笑外国人或者表示音效而已。这是除了“完全无意义说”以外唯一被专家所接受的假说。然而，在进行分析时，科拉鲁索并不知道研究古希腊花瓶的专家已经多次判断出这些文字属于无意义的文字，因此，上述意见并不会影响他的判断。

既然梅厄认为这些看似无意义的文字代表的是用希腊语写成的外语名字，那么我们就有必要研究一下塞西亚人的名字过去（以及现在）具有哪些特点。事实上，塞西亚人一共有两种名字，一种是私有名，另一

种是公开名。公开名通常是以这个人的性格特点，或者小时候的某种事迹为基础的。关于这一点，梅厄等人举出了以下的例子：

> 某个家庭的公开名可能是“上帝让你活着”（在塞西亚语中的意思等同于“谢谢”），因为这个家族的某个祖先因总是彬彬有礼而被人熟知。其实，一些现代的高加索语昵称也是这样得到的：比如“corpse-cause-die”意为“打一匹死马”，形容一个人的性格极其固执。“dog-shit”意为“狗屎”，这个昵称描述的是一个人小时候曾经踩到狗屎的经历。而“stuck in the oven”意为“卡在炉子里”，这个昵称描述的是一个人小时候曾经爬到冷的炉子里并且被困住了。㊟

这些昵称可都不怎么体面。但是，严肃地说，有些人的名字还是很体面的。既然我们已经知道这些昵称大概是在什么范围了，现在我们不妨来看看科拉鲁索的分析结果。

案例1（公元前510—前500年）：

> 一位塞西亚弓箭手旁边写有“ΧΥΧΟΣΠΙ（Khukhospi）”的字样。科拉鲁索认为这是古阿布哈西亚语，意思为“热情的呼喊者”或者“战斗的口号”。这个名字真是比“狗屎”好多了呢！

案例2（公元前525—前500年）：

> 一位亚马孙女战士旁边标有“ΠΚΠΥΠΗΣ（Pkpupes）”的字样。科拉鲁索认为这是尝试模仿古切尔克斯语的一种写法，意思是“值得穿戴盔甲”。

案例3（公元前510—前500年）：

三个正在备战的亚马孙女战士的名字分别是“Andromache”、“Hyphopyle”，以及“Antiopea”。其中第三个名字“Antiopea”还标有“XEϒXE”的字样。在上文中我们曾提到，某些无意义的文字中会重复出现字母X（chi）来取笑外国人，这段文字看起来就是一个例子。但是“kheukhe”是古切尔克斯语“英雄之一”或者“女英雄之一”的意思。

案例4（公元前525—前500年）：

一位亚马孙女战士或者塞西亚人（性别不明确）被标记为“ΣΕΡΑΓϒΕ（Serague）”。在古切尔克斯语中，这个词的意思是“佩有匕首或者剑”。

案例5（公元前510—前500年）：

赫拉克勒斯和一名亚马孙女战士在一起。这名亚马孙女战士被标记为“ΒΑΡΚΙΔΑ（Barkida）”。在古切尔克斯语中，这个词是“公主/高贵的女性亲属”的意思。

案例6（公元前475—前450年）：

一位亚马孙女战士被标为“ΓϒΓΑΜΙΣ（Gugamis）”，也就是古切尔克斯语中的“铁”。另一位亚马孙女战士被标为“ΟΙΓΜΕ（Oigme）”，这个词像是尤比克语，大概意思是“不要失败！”

案例7（公元前525—前510年）：

一个花瓶上有两位亚马孙女战士和一只狗。花瓶上有“OHE（Υ）N”和“KE（Υ）N”的字样，科拉鲁索认为这是古阿布哈西亚语，第一个词的意思为“她/她们曾在那儿”或者“我们在互相帮助”，而第二个词的意思为“把狗松开”。注意，在进行上述分析的时候，科拉鲁索并不知道花瓶上有狗的图案！

案例8（公元前550—前530年）：

在花瓶上，赫拉克勒斯在和亚马孙女战士作战。亚马孙女战士被标记为“ΓΟΓΟΙΟΙΓΙ”和“ΓΟΓΙϜΙΚΙ”。科拉鲁索认为“gogoioigi”和“gogiwiki”表示格鲁吉亚语的“处女”一词。

案例9（约公元前550年）：

花瓶上，赫拉克勒斯又在和亚马孙女战士作战，但是这一次他得到了忒拉蒙和其他希腊战士的帮助。其中四位女战士被标上了希腊名字，而第五位女战士被标为“ΚΕΠΕΣ（Kepes）”。这个词像是古阿布哈西亚语，意思为“热情的（女）性”。我开始理解为什么其他战士这次都要来帮助赫拉克勒斯了！

案例10（公元前550—前500年）：

赫拉克勒斯又在和亚马孙女战士作战了。其中一位女战士被标上了希腊名字，另一位被标为“ΟΑΣ ΟΑΣ（oas oas）”。这个词听起来像是奥塞特语中的词，意思是“神圣的”或者“神灵的”。所以，这次赫拉克勒斯只能孤军奋战了。

案例11（约公元前510—前500年）：

花瓶上画着一位希腊公民战士，他手上拿着一些内脏。花瓶上展示的不是战斗后的场面，而是出征前占卜吉凶的场面。一个男孩手中拿着更多的内脏，一位塞西亚弓箭手越过他的肩膀看向内脏。另外还有一个女人也在观看这一切，此外，还有一只狗。花瓶上的文字不是希腊语，但是在古切尔克斯语中却有意义。男孩旁边写着“TΛETϒ（tletu）”，意思是“跳跃者”；公民战士旁边写着“ITEIΣ（iteis）”，这个词表示位置，意思是“站在这里的是一位战士”；狗旁边写着“EIOΣ（eios）”，这个词也是表示位置的，大概意思是“狗站在他旁边”；女人旁边写着“IΣΛEI（islei）”，意思是“我给他穿上（盔甲/衣服）”。

案例12（公元前510—前500年）：

花瓶上一边画着3位神，这3位神都标有希腊名字；另一边画着一位希腊战士、一位塞西亚弓箭手、一只狗，以及一位老人，并标出了5个无意义的词。下面我们来逐一分析这5个无意义的词：塞西亚弓箭手的头后方标有“KIΣI（kisi）”一词，在古切尔克斯语中，这个词的意思是“这里是他的朋友”；塞西亚弓箭手的头右方标有“ΓEXΓOΓX（gekhgogkh）”，在古阿布哈西亚语中，这个词的意思是“勇敢的敌手”；在狗的上方的单词缺了一个字母，这个词看起来像是“XΛE[.]ΣI（khle[.]si）”，科拉鲁索未能分析出这个词的意思；在老人的背后写着“XΛEIOΠXIO（khleiopkhio）”，这似乎是古切尔克斯语，意思是这位老人是“一个大人物的女儿”的后人。

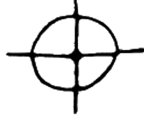
我把案例12中最令人震惊的一个词的解释留到了最后。在案例12中，还有另一个看起来无意义的词“XEXΓIOXEXOΓE（khekhgio-

khekhoge）”。在这个词中，字母X（chi）在同一个词中出现了4次。在上文中我们提到，在很多无意义的文字中，同一个词中“kh”会多次出现，这就是其中一例，这么奇怪的词肯定是没有意义的！那么，这个词会不会是用来嘲笑外国人的呢，就像在希腊的戏剧中经常出现的情况？好吧，这种情况不太可能成立。因为这个词没有出现在塞西亚人的旁边，而是写在希腊战士的背后。此外，在一个词中出现4次“kh”音节的情况在古切尔克斯语中确实存在。实际上，在古切尔克斯语中有7种不同的读音都被希腊人以“kh”做近似表示，因为在希腊语中这7种读音没有办法明确区分。事实上，在古切尔克斯语中，“khekhgio-khekhoge”的意思是“从勇士中选出来的一个”。

注意，古切尔克斯语方言一共只有2~3个元音，但是却有48~81个不同的辅音。因此，一般来说，古切尔克斯语的读音比希腊字母能够表达的读音更多。所以，希腊人不得不用同样的希腊字母来表示古切尔克斯语中的不同发音。所以，当古切尔克斯语被翻译为希腊语时，同样的字母会在一个词中反复出现，而在古切尔克斯语的原文中其实是不会出现这种情况的。

上面的情况使我们产生了一个疑问，那就是：当我们把希腊字母重新翻译回古切尔克斯语时，会不会面临过多的选择呢（也就是翻译的灵活度过高，或者主观发挥余地太大）？虽然每一个希腊字母可以被翻译为不同的古切尔克斯语字母，但也许我们总是可以找到适合的古切尔克斯语词。梅厄考虑到了这个问题（也许她甚至考虑到其他学者会因为这一点反驳她的结论），所以她又进行了另外一项测试。

对照实验



为了搞清楚科拉鲁索的解读是不是作者的原意，梅厄进行了一项对照实验。在这项对照实验中一共有两组文字，第一组“无意义”文字来自绘制有亚马孙女战士或者塞西亚人图案的古希腊花瓶，而第二组“无意义”文字来自一些既没有亚马孙女战士，也没有塞西亚人图案的花瓶。因此，第二组中的文字不应该与科拉鲁索熟知的这些语言有关。

这项对照实验的结果相当令人满意。梅厄共向科拉鲁索提供了10条文字作为第二组（对照组）的样本，科拉鲁索给出了以下10条回答[注]：

1. “垃圾。”

2. “xargekexs一词也许有希望被破解出来，但是没有什么明显的解释。”

3. “也许是希腊方言？”

4. “可能是古巴尔干语？或者伊利里亚语、默西亚语、马其顿语、色雷斯语？”

5. “完全看不懂。”

6. “看起来像是胡言乱语。”

7. “无法理解，我不熟悉，有些看起来像是希腊语，但是词的结尾十分奇怪。”

8. “我没有办法分析出任何意思。”

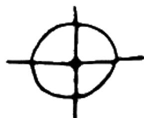
9. “其中三个字母可能是古阿布哈西亚语中‘我们’的意思，但是整体意思看不懂。”

10. “总的来说这些看上去像是胡言乱语，莫名其妙，无法解读，除非这些语言描述的是饮酒或者跳舞的情况。”

也就是说，对于这些科拉鲁索不熟悉的语言文字，他确实绝大多数都没看懂。有趣的是，上面的第10条文字所在的花瓶上确实描绘的是饮酒宴乐的场面。

在上面的实验中，实验组的文字被解读出了一些合理的意思，而对照组的文字则几乎都没有办法解读。这两个现象说明，上述实验的结果非常具有说服力。梅厄团队中的古希腊花瓶学家桑德斯表示："有了这个结果，以后我在把某些文字判断为无意义文字之前可一定要多加小心了。"㊟

亚马孙女战士真的存在吗？

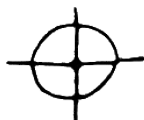


关于亚马孙女战士的描述首次出现于《伊利亚特》中。在不久之前，学者们还认为亚马孙女战士是一个只存在于神话中的虚构民族。然而，专家以前还认为古希腊花瓶上的这些所谓"无意义的文字"不可能包含任何的含义呢。现在，已经有研究结果显示，这些绘制有亚马孙女战士和塞西亚人的花瓶上的文字实际上是有意义的，因此，下一步的问题也就产生了。在梅厄的著作《亚马孙女战士：古代世界中的女战士的生活和传奇》（*The Amazons: Lives and Legends of Warrior Women across the Ancient World*）中，梅厄不仅提出了这个问题，还对这个问题做出了回答：

> 但是，亚马孙女战士是真实存在过的吗？虽然很长一段时间以来，专家们一直相信亚马孙女战士完全是虚构出来的，但是现在已经有大量确切证据证明，古希腊以及其他古代传说中的亚马孙女战

士事实上很大一部分来自历史上的真实事件。被古希腊人称为“塞西亚人”的草原游牧民族善于骑马，而且女人过着和男人一样艰辛的户外生活……考古学证据显示，在这个草原游牧民族中，每三到四个女人中就有一个女人生前曾参加过战斗，并和她生前所用的武器埋葬在一起。注

悬而未决的问题



梅厄、科拉鲁索和桑德斯所做的工作非常优秀，但是其他学者也没有必要感到绝望，因为在这个领域中还有许多问题目前尚未探明。比如，《怜子门农图》的问题仍未解决，我们仍然不知道这幅图上的文字“EENEMEKNERINE”究竟是什么意思。

另一个例子见于一个古希腊的杯子上。这个杯子是20世纪30年代在阿提卡中部的一个名为科罗皮的村落中被发现的。1945年，尤金·范德普尔（Eugene Vanderpool）发表了一篇关于这个杯子的论文，称这个杯子被发现时已经碎成了很多块，但出土后被重新拼合修复，修复者用胶泥代替了缺失的碎片。目前，这个杯子属于某个私人收藏的一部分，从下页的图2–4和图2–5中可以看到它的样子。

杯子上有一个男性的形象，这个男人旁边标有“ OИƎИOIƎИ ”的字样，这个词中字母的方向是反的，范德普尔认为这些都是无意义的文字。此外，杯子上还有一个女性形象，旁边标有“KNIONI”的字样，范德普尔认为这也是无意义的文字。女人的旁边还有另一个词“KAVITINE”，被认为是一个女子名，比如“Καλλιτίμη”之类的名字。有没有人能得出比这更好的解答呢？如果有人能搞清楚这些文字

的含义，这个杯子也许会告诉我们一些小故事。我们也许可以通过这个词中字母的特殊规律来确定“ OИƎИOIƎИ ”的意思。哪一个希腊语单词中的字母符合这种特殊规律呢？这个杯子上的文字是否有可能是某种外国语言，而在这种外国语言中这个词是有含义的呢？在本书的第1章中，我们已经讨论过单词中的字母规律以及这些规律在密码分析中的价值。在对这个杯子上的文字进行分析的过程中，这方面的知识同样可能具有很高的价值。



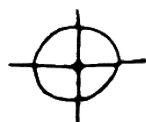
图2-4 包含无意义文字的阿提卡杯子



图2-5 上述杯子的局部细节图，图中包含两段无意义的文字

有些花瓶的画家会在不同的花瓶上多次使用同样的无意义文字，每一个字母都完全相同。这些画家包括萨福绘制者（重复了lilislis、loloslos、etotot）、古列尔米绘制者，以及尖鼻子绘制者注。如果这些无意义文字真的毫无意义的话，这些艺术家们为什么要花费精力保证每个花瓶上的文字完全一样呢？为什么不在绘制每个花瓶的时候随机编造一些不同的文字呢？

对未来破译工作的反思和想法



现在，让我们来回顾一下梅厄的团队到目前为止取得的研究进展，并且了解一下该团队所设想的未来发展方向，我认为这个反思过程是非常有趣的。严格来讲，梅厄团队研究的这些花瓶上的名字并没有经过加密，这些名字的表示方法很明显，连一个词汇量有限的古希腊人也能够

看得懂。然而，这些名字仍然能以很多方式与密码产生联系。首先，梅厄解释道：

> 我之所以会对破译古希腊花瓶上的这些貌似无意义的文字产生兴趣，部分原因在于我的第一段婚姻。在越南战争期间，我曾与一位在陆军安全局工作的密码学家结婚，他曾先后在英国北约克郡哈罗盖特附近的皇家空军曼威斯山基地、美国国家安全局的情报收集点，以及美国国家安全局位于华盛顿特区附近的米德堡分部工作过。㊟

接下来，某些读者可能已经注意到，这种加密方式与恺撒所使用的以希腊字母表加密拉丁文的方式十分相似。总的来说，在破译一些意义不明的古代文字的过程中，经常会用到一些与密码分析技术完全相同的技术（即使书写这些文字的人并没有打算隐藏文字的意义）。

在梅厄团队的论文发表之前，作者对论文进行了一处改动。从这处改动中，我们也可以看出这项工作与密码之间的联系。在论文2012年的第2版中，作者写下了以下内容：

> 目前存在许多可能非常有趣的“无意义的文字”。在这篇论文中，我们只考虑了其中一小部分。在未来的研究中，我认为我们可以设计一些统计检验，来判断这些无意义文字中的字母分布是不是从整个希腊字母表中随机选择的，还是有某些特殊的音或者辅音字母出现的概率更高，如果存在这条特征，就可能是高加索语或者某种其他语言。这些工作也许可以由一个考古学家/花瓶专家以及数学家组成的团队来完成。……另外，我们还可以进行另一项统计研究，即研究不同主题文物上出现的无意义文字中的字母分布在统计上是否有区别，比如与外国情境相关的无意义文字，和其他情境（比如神话情境）中的无意义文字。㊟

然而，在2014年发表的这篇论文的最终版中，作者却没提到数学家的贡献。梅厄解释了做出上述改动的原因：

> 由于4号匿名评论者的评论，我们修改了上述段落，删除了希望考古学家/花瓶专家以及数学家合作研究这些无意义的文字的内容。在此，我将全文引用这位4号匿名评论者的评论，因为我认为他的评论可能具有一定的价值。4号匿名评论者指出："在论文的结尾，作者提出了一些可能的统计分析。我建议通过以下这些方式做出修改。第一，我认为考古学家/花瓶专家应该选择的合作对象不是数学家，而是计算语言学家，因为和数学家相比，计算语言学家更善于处理文字的统计分析。第二，虽然我明白作者提出的这些统计测试只是一种实验性的假想，但我对作者建议的这些分析方法能否产生有价值的结果表示怀疑。作者研究的这些无意义文字的长度都很短，因此关于这些无意义文字的资料相对有限。当然，我们拥有大量相关的希腊语文字样本（虽然其中大部分都是经过重新修正后的版本），但是同一时段其他语言文字的样本却不多，因此我们只能使用那些现代版本的语言来作为我们分析的依据。由于以上两点原因，我认为作者提出的统计研究会产生有价值结果的可能性不大，所以如果这个研究确实产生了有价值的结论，我将感到十分惊讶。然而，如果能够找到合适的人合作的话，我想作者提出的这些统计方法还是值得尝试的。"[注]

梅厄写道："在这篇论文的第2版中，我们将继续维持关于与数学家合作的原始建议不变。但在发表至《西方之国》（*Hesperia*）期刊的版本中，我们对这段内容进行了修改。"[注]

4号评论者的评论提道："和数学家相比，计算语言学家更善于处理文字的统计分析。"这段评论具有一定的讽刺意味，因为要论对文字做统计处理，密码分析学家才是这个领域的真正先驱。此外，美国国家安全局是世界上雇用数学家最多的机构，而国家安全局的工作任务从本质

而言就是与密码相关的，并且涉及大量针对文字信息进行的统计分析。

在这篇论文的最终版本中，作者仍然提到了一些关于未来研究工作的想法，这些想法显然仍与数学有关：

> 如果这些所谓的“无意义的文字”真的是随机的胡言乱语，这些艺术家可能会使用希腊字母表中的所有字母。[注]

这篇重要论文的第2版和最终版之间还有另一处区别，那就是：在最终版本中，作者降低了对无意义文字数目的估计值。

这篇论文的第2版中写道：“在古希腊的花瓶上出现过超过2 000处无意义的文字（即没有意义的希腊字母串）。”而在这篇论文的最终版本中，作者称这些无意义的文字只有“1 500多处。”之所以会出现这样的区别，是因为在“如何对无意义的文字进行计数”的问题上存在一些分歧。由于存在一些无法区分的案例，作者最终决定还是用了一个较低的估计值。然而，即便古希腊花瓶上的无意义的文字只有1　500处，这也给这方面的进一步研究提供了巨大的空间！

我们可以看出，梅厄团队的这篇论文还远没有为这个领域的研究画上圆满的句号。梅厄、科拉鲁索和桑德斯只是为我们打开了一扇门，如果其他学者愿意以更加开明的头脑来审视这一领域的话，未来很可能会涌现更多新的研究成果。

研究者们大可不必担心梅厄的团队已经解决了这一领域中“最容易”的问题。目前，大约有140个阿提卡花瓶上同时出现了有意义的文字和无意义的文字。[注]我相信，有些读者肯定希望对这方面的内容自行探索，因此我希望向读者提供一份阿提卡花瓶的参考列表。然而，我很快发现，市面上存在大量关于阿提卡花瓶的列表，而且这些列表通常都不够完整。因此，我发信给戴维·桑德斯，问他这些阿提卡花瓶的参考列表中究竟哪一份最好。他做了以下回复[注]：

亲爱的克雷格，

这方面最好的资源（至少对搜索而言是最好的资源）来自鲁道夫·瓦赫特（Rudolf Wachter）的阿提卡花瓶铭文计划（Attic Vase Inscriptions project，简称AVI计划），该资源可以在以下网址找到：www.avi.unibas.ch。

以上的数据库是在亨利·伊默瓦尔的《阿提卡花瓶铭文资料》（Corpus of Attic Vase Inscriptions）的基础上建立起来的。该资料已经收入比兹利档案数据库（Beazley Archive Database，http://www.beazley.ox.ac.uk/databases/inscriptions.htm）。就已出版的资料而言，伊默瓦尔的著作和论文是优先推荐的：

Immerwahr，H.1990. Attic Script：A Survey，Oxford.

___. 2006. “Nonsense Inscriptions and Literacy，” Kadmos 45，pp. 136–172.

___. 2007. “Aspects of Literacy in the Athenian Ceramicus，” Kadmos 46，pp. 153–198.

希望以上内容可以为你提供帮助。如果还有其他问题，尽管联系我。

戴维

会编码的维京人



虽然在流行文化中，人们倾向于把维京人想象成一群崇尚暴力、缺乏智力的人，但是实际上维京人写密码的水平一点儿也不比古希腊人

低。为了验证这一点，我们不妨看看瑞典的罗特布鲁纳石（Rotbrunna Stone），这块石头来自公元1000年。在图2–6中可以清楚地看到石头上的图案。

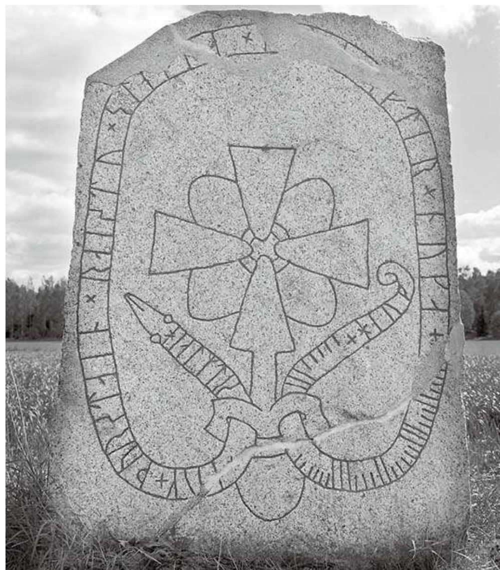
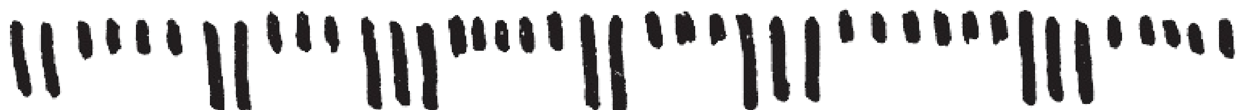


图2-6 瑞典的罗特布鲁纳石

我们可以注意到，在靠近蛇尾的地方有许多长线和短线。我将这些长线和短线复制如下，其中距离蛇尾较远的线放在左侧，距离蛇尾较近的线放在右侧：



注意，上面这些线条看起来并不是随机的。它们出现的规律是一组长线后面跟着一组短线。如果我们计算每组的线条数量，就会得到以下数字：

2, 4, 2, 3, 3, 5, 2, 3, 3, 6, 3, 5

然后，我们可以把上面这些数字两两配对，就得到：

24, 23, 35, 23, 36, 35

读者是否发现这些数字看起来像是用波利比奥斯密码加密过的呢？如果你有这样的想法，那么你就对了，因为维京人确实使用了这种方法！在几个世纪里，维京人至少曾用两种不同的方式把他们所使用的如尼文字母排列在网格中。有了这种网格的帮助，维京人就可以轻松地完成加密工作。

图2-7 维京时期的网格（含24个字母）和维京时期的网格（含16个字母）

有时，这样排列的如尼文字母被称为“alphabet”（字母表），然而这种说法并不准确。“alphabet”来自希腊字母表的前两个字母alpha和beta。我们同样也可以用这个词来称呼拉丁文字母表，因为拉丁文字母表以字母A和B打头，而A和B这两个字母其实就对应希腊文字母表中的alpha和beta。然而，如尼文字母表的顺序却完全不同，因此这类字母表通常被称为“如尼行”或者“fuþark”（futhark）。这个词语也是由如尼文字母表中的前几个字母组合而成的（如尼文字母表共有两种形式，即旧式和新式）。由于如尼文字母表有各种不同的形式，所以有时研究者也把这种字母表称为fuþorc（futhorc）（指如尼文字母表的“盎格鲁–弗里斯兰”形式，或称“中世纪”形式）。在如尼文字母表中，“þ”被音译为“th”，因为这个字母的发音类似于英文中“th”的发音。

为了完全破译上面的密码，我们需要用到图2–7中右边网格的一个修订版。在我们所要用到的这个字母表中，行的排列方式与如尼文中行的排列方式有所不同。

每行的字母

行	1	2	3	4	5	6
3	f	u	(th)	ą	r	k
2	h	n	i	a	s	
1	t	b	m	l	R	

图2-8 维京字母表的一种变化形式

有了图2–8中的这个字母表以后，我们就可以把这段密码破译如下：

24,	23,	35,	23,	36,	35
a	i	r	i	k	r

结果为airikr或者Erik（一个男子名）。

维京密码的另一个例子是瑞典的勒克石（Rök stone，参见图2–9）。

勒克石上出现了多种加密形式。其中一部分密码的密钥如图2–10所示。

在这段密码中，如尼文字母表被分为三组，或称三行。为了破译这段密码，我们把每组中的各个字母分别向前移动一位。字母的对应关系

如下：

a i r f b f r b n h n **变为：** s a k u m u k m i n i

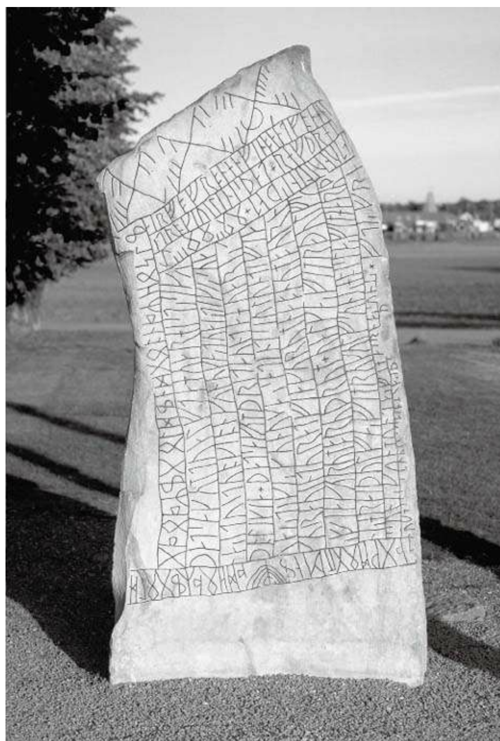


图2-9 高达13英尺的瑞典勒克石

III	II	I
ᚠᚢᚦᚬᚱᚴ:	ᚼᚾᛁᛅᛋ:	ᛏᛒᛘᛚᛦ
f u þ ą r k	h n i a s	t b m l R
1 2 3 4 5 6	1 2 3 4 5	1 2 3 4 5

图2-10 位于瑞典东约特兰的勒克石上的部分密码的密钥

结果为sakum ukmini，即I say to the youth / I tell the young（我告诉年轻人）。

另一种解读（在第二个词首加上字母m）结果是sakum mukmini，即I tell the great memory（我告诉伟大的记忆）。

读者也许会觉得我在这段话中添加了一个m有点儿作弊，但是这种做法是完全合理的。在书写的时候，维京人会遵守这样一个规律：如果某个单词的首字母与之前单词的末字母一致，就把后一个单词的首字母略去不写。读者需要根据上下文的内容来决定此处是否有字母被省略。

维京人的这种加密方式还有许多变种，比如，有时他们会把每个字母向前移动一到两位。我们知道，恺撒曾使用过这种著名的加密方法：把字母表中的每个字母都向后移动3位。因此，虽然这种字母移位的加密方法在今天的我们看来也许很简单，但是就连著名的军事人物恺撒也没有发明出更高明的加密方法。今天，我们把所有这类密码（即将字母表中的字母统一移动某个固定位数的密码）统称为“恺撒移位密码”。

事实上，维京人的密码水平已经超过了我们目前所知道的古希腊人和古罗马人的密码水平。为了说明这一点，让我们来考虑勒克石上的另一处密码。维京人在巨石上刻字的时候，不仅会在石头的正面和反面刻上字，还会在石头的顶部和侧面刻上字（参见图2–11）。

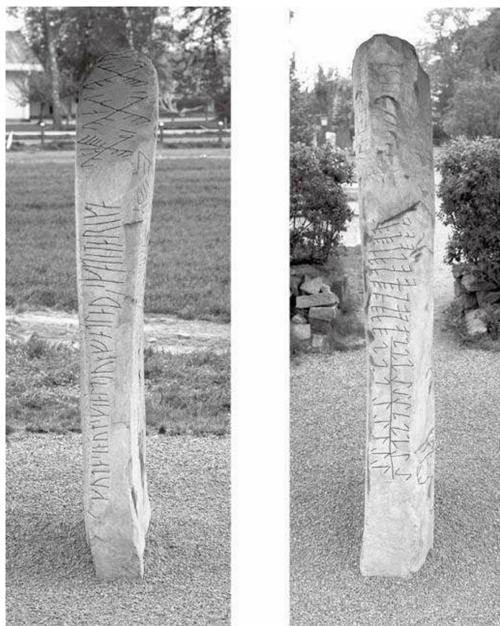


图2-11 从更多角度看勒克石

虽然勒克石上的如尼文字母有一定程度的损毁，但是损毁程度并不高，因此专家仍然能够填补缺失的字母。图2–12是勒克石一个侧面上的文字。

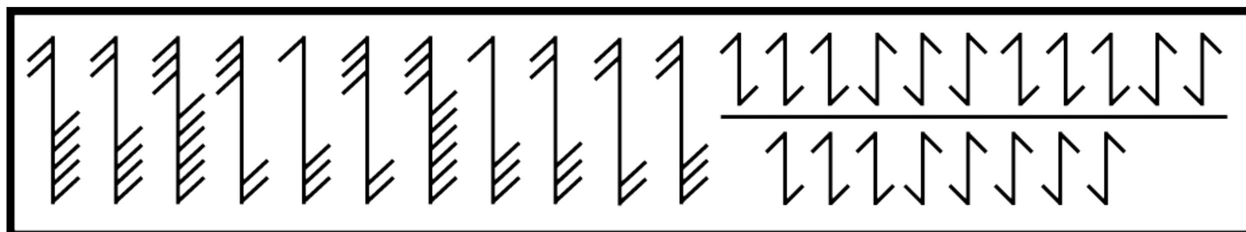


图2-12 勒克石上的另一段密码

如果我们把这些图案当作波利比奥斯密码的一种特殊形式，我们就可以把这些装饰图案翻译成数字，然后再把这些数字转化成有意义的文字。

25 24 36 32 13 32 36 13 23 22 23 - 33 32 35 =

s a k u m u k m i n i th u r

最后，我们得到的密码明文和上例中的密码明文内容一样。

上面这些图形的特点是：一条竖线两侧以一定角度伸出了很多短线。有时候，两条竖线可以交叉在一起，这样就能一次表示两个字母。在图2–11中左侧石头的上部可以看到这种交叉的竖线，在图2–9的上部也可以看到这种交叉的竖线。



图2-13 加密后的字母对（为了让读者能看得更清楚而重新绘制的版本）

除了上面这些密码形式以外，维京人还有其他形式的密码（参见图2–14）。如果读者对波利比奥斯密码不熟悉的话，可能会认为图2–14中的这些图案只是在描绘鱼、某种设计图形、人，或者有胡子的男人，而不会想到这些图案背后还有其他意义。而事实上，图2–14中的这些图形

可以用密码的形式传达加密者想要传达的任何信息。

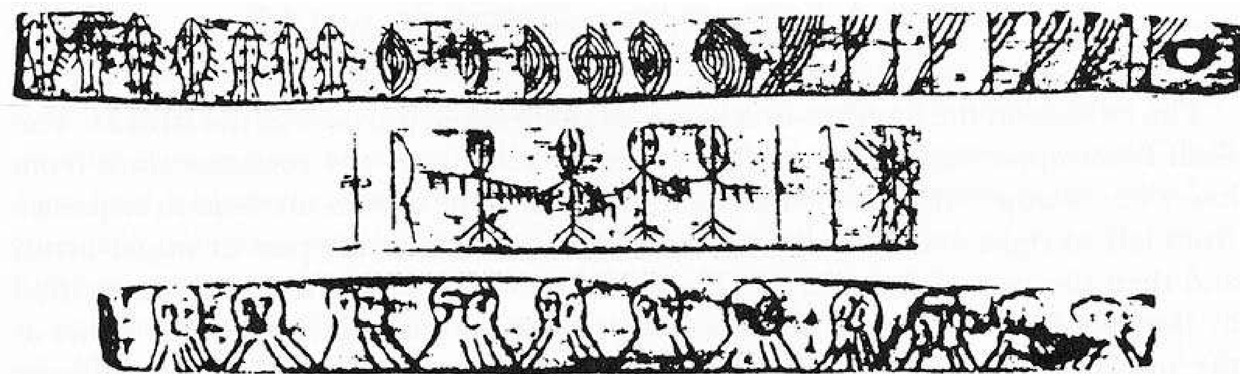


图2-14 维京人制造的木棍上刻的图案

上方这根木棍上的密码破译后为："上帝给予我们……"中间这根较短的木棍上的密码破译后为"Klim"，这几个如尼文字母是"圣克莱门特"一词开头的几个字母。而底部的木棍上的密码破译后为"作为一个人的生活（as one's life）"。注

上面这些密码有一个共同特征，那就是读者甚至很难发现它们是隐藏着某些信息的密码。我们把这种形式的密码称为"隐写术"（steganography）。好几个世纪以来，隐写术以各种各样的形式出现，比如隐形墨水、微小的点，或者数字图像中隐藏的信息［对于最后一种形式的"隐写术"，读者可以参见《未解之谜（下）》第9章］。

至此，我们已经初步了解了维京人所使用的密码技术的范围，并且见识了这些维京密码的微妙之处。现在，我们来研究另外一块石头上的文字，这些文字一般被认为是无意义的文字。

斯蒂格·埃利亚松（Stig Eliasson）写道："在斯堪的纳维亚维京时期/中世纪早期的如尼文文献中，有一小部分文字虽然看似是用正常的自然语言写成的，其意思却无法被解读。现代的如尼文专家几乎一致认为这些文字（以及其他一些更加不正常的文字，如可能是古人习字产生的文字）在语言学上是没有意义的。"注

但是，埃利亚松认为，丹麦的瑟鲁普（Sørup）符文石上的文字是

有意义的。符文石上的文字看起来的确不像是一个不识字的工匠的作品。根据埃利亚松的描述，这块石头上刻有“经过精心设计的、风格优雅的丹麦文字” 注。他提出了一些证据来说明石头上的文字是巴斯克语。如果埃利亚松的结论正确，那么这一研究成果和前文提到的梅厄团队的研究成果性质非常相近。

符文石上的文字刻得非常认真，需要指出，这种情况在当时比较常见。在某些如尼文铭文中，我们确实发现过雕刻者错刻的情况，但是这种例子极为少见。

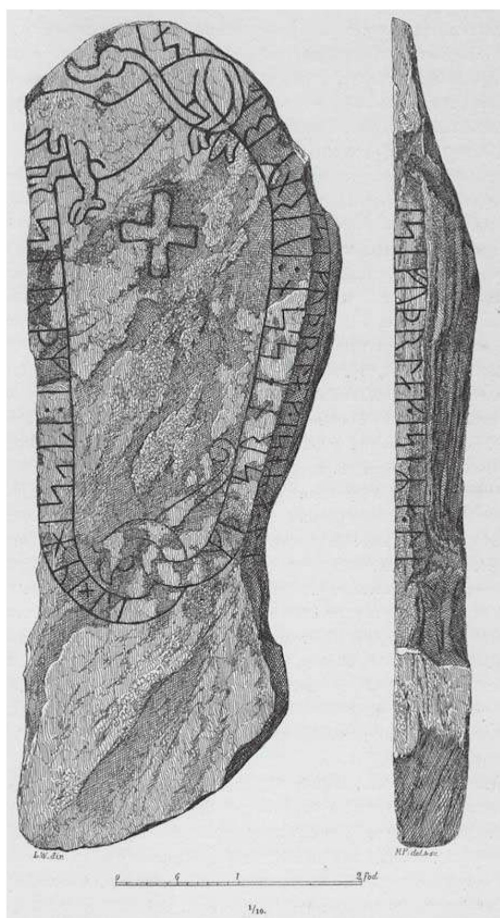


图2-15 丹麦的瑟鲁普符文石，编号DR 187，公元1050—1250年

如果我们在这些如尼文铭文中只能找到两种极端的情况——要么是完全无意义的文字，要么是几乎完美的文字，那么我们似乎就会得到这样一个结论：这些如尼文铭文的雕刻者要么完全不识字，要么文化水平

非常高。这是一种非常奇怪的现象。为什么就没有文化程度中等的雕刻者呢？在某些例子中，即使石头上没有雕刻者的签名，专家也可以通过一些方式来确认不同的石头是不是同一位雕刻者的作品。然而，在所有例子中，我们没有发现任何一位雕刻者一开始会雕刻一些无意义的文字，在学会了读写之后，便雕刻出有意义的文字。

这种在石头上刻上“无意义的文字”的例子还有很多，在图2–16至图2–25中我列出了其中10个例子。

迈克尔·P.巴恩斯（Michael　P.Barnes）对编号为U　811（参见图2–20）的文字做了以下评论：



图2-16 U 370



图2-17 U 466



图2-18 U 468

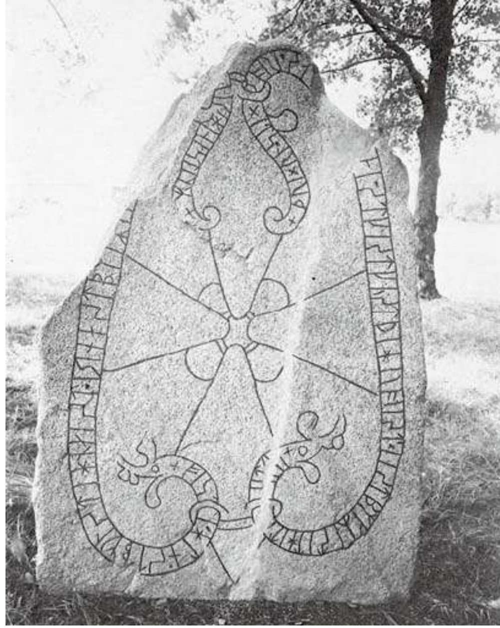


图2-19 U 483



图2-20 U 811

某些符文石上的文字看起来没什么神秘的，但是内容却无法解读，或者部分无法解读。在瑞典的乌普兰发现的11世纪的耶尔斯塔铭文就提供了一个这样的例子。这段铭文的内容是：“**fast...R:þuliak: oaRtþiol:atiurai:fasatiR:þaloi:oaRfsai**”。这串字

符中几乎没有一个可辨认的斯堪的纳维亚语单词。许多人尝试在这段铭文中寻找某种隐藏的信息，他们这么做的原因之一是，这段文字虽然意义不可理解，却雕刻得非常完美。然而，目前还没有任何人能够成功破译这段铭文的意思。在这个例子以及其他一些相似例子中，雕刻者也许认识如尼文字，却不知道（或者基本不知道）如何使用如尼文字来书写语言（并且要么无法寻求帮助，要么不愿意寻求帮助）。此外，这种无意义文字的出现似乎还说明，这些文字的委托人也不识字，因此委托人无法检查雕刻的内容是否正确。注



图2-21 U 835



图2-22 U 983

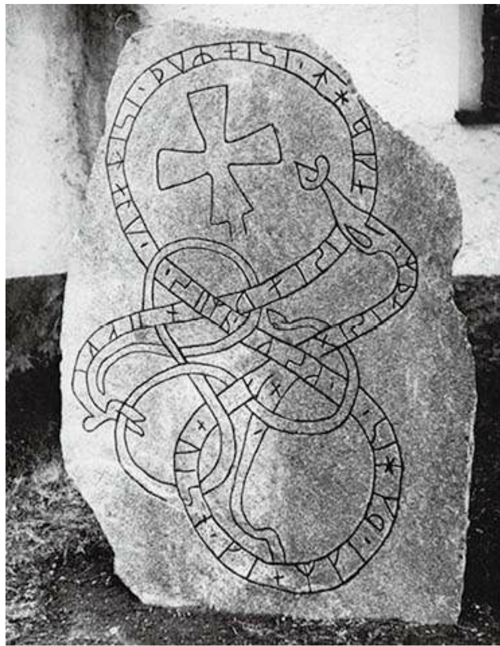


图2-23 U 1061

的人来帮他检查雕刻的文字是否正确。



图2-24 U 1125 A面



图2-25 U 1125 B面

然而在我看来，即便委托人自己不识字，他也很容易找到一个识字的人来帮他检查雕刻的文字是否正确。

值得注意的是，以上10块石头都是在一个相对集中的区域发现的，即瑞典的乌普兰地区。

如果要详细讨论这些石头上的所有文字的话，恐怕要单独写一本书才行。目前，还没有这样的书籍面世。事实上，对其他种类的如尼文字的调查研究目前也存在严重的空白。迈克尔·P.巴恩斯指出：“目前，以下这几类如尼文字尚没有语料库，其中包括盎格鲁–撒克逊如尼文、弗里斯兰如尼文、格陵兰如尼文和马恩岛如尼文。”[注]

如尼文可以用来表达一系列语言，大多是日耳曼语族的语言（比如古英语和古挪威语）。但是，我们也知道它还可以用来表达拉丁语、希腊语，以及希伯来语的情况。不管埃利亚松关于丹麦的瑟鲁普符文石的论断是否准确，都存在这样的可能性：也许在未来的某一天，我们会发现，目前被认为是无意义的文字的某些如尼文事实上代表的是一种我们没有预想到的语言。

某些目前被认为是无意义文字的如尼文其实有可能是某种密码，迈克尔·P.巴恩斯在他的评论中其实无意识地提供了支持上述观点的证据。巴恩斯指出：“ᛇ这个字符很少出现在有意义的文字中。”[注]为什么要加上“有意义的”这个定语呢？如果ᛇ很少出现，为什么巴恩斯不直接说“ᛇ这个字符很少出现在文字中”呢？巴恩斯的修辞方式表明，这个字符出现在“无意义的文字”中的概率大于其出现在有意义的文字中的概率。

所有密码系统（除了纯粹的换位重排系统以外）都会改变字母出现的频率。在一段加了密的英文中，字母E出现的频率可能小于12.7%，而字母Z出现的频率可能大于0.07%。也就是说，在通过替代法加密而得的密文中，常见字母出现的频率会降低，而不常见字母出现的频率会增高。事实上，巴恩斯的上述评论说的正是后一种现象。

对于目前无法解读的如尼文，我们需要将相关的石头（比如瑞典乌普兰地区发现的石头）归为一组，对该组石头上雕刻的所有无意义的文字进行统计分析，以判断这些文字是否有可能是用某种相同的加密方法

产生的密文。如果不同石头上的无意义文字的字母出现频率彼此间相一致，并且都与可解读的如尼文的字母概率不同，那么我们就有很充分的理由认为这些“无意义”的文字的背后其实隐藏着某种意义。

---

1. Thomas Hoving, False Impression: The Hunt for Big-Time Art Fakes (New York: Simon & Schus-ter, 1996), 52–53.
2. Mary-Ann Russon, “Tiny Egyptian Mummy Confirmed by CT Scan to be Baby’s Remains,” Inter-national Business Times, May 8, 2014.
3. 马斯塔巴是一种古埃及的墓葬建筑类型。——译者注
4. W.M.Flinders Petrie, Ten Years’ Digging in Egypt 1881–1891, 2nd ed. (London: The Religious Tract Society, 1893), 124–25.
5. W.M.Flinders Petrie, Illahun Kahun and Gurob, 1889–90 (London: David Nutt, 1891).
6. Alan R.Schulman, “The Ossimo Scarab Reconsidered,” Journal of the American Research Center in Egypt 12 (1975): 15–18, p. 16 quoted here.
7. John Coleman Darnell, The Enigmatic Netherworld Books of the Solar-Osirian Unity, Cryp-tographic Compositions in the Tombs of Tutankhamun, Ramesses VI and Ramesses IX, (G.ttin-gen, Germany: Academic Press Fribourg, Vandenhoek & Ruprecht, 2004), 1–2.
8. 孔苏（Khonsu）是古埃及神话中的月神。——译者注
9. étienne Drioton, “Les principes de la cryptographie égyptienne,” Comptes rendus des séances de l’Académie des Inscriptions et Belles-Lettres, 97e année, no. 3 (1953): 355–64.
10. John Coleman Darnell, The Enigmatic Netherworld Books of the Solar-Osirian Unity, Cryp-tographic Compositions in the Tombs of Tutankhamun, Ramesses VI and Ramesses IX, (G.ttin-gen, Germany: Academic Press Fribourg, Vandenhoek & Ruprecht, 2004), 5.
11. Alan R.Schulman, “The Ossimo Scarab Reconsidered,” Journal of the American Research Center in Egypt 12 (1975): 15–18, p. 16 quoted here.
12. 五长官指古代斯巴达每年由全体公民选出的五位督政官，负责协助国王执政。——译者注
13. Plutarch’s Life of Lysander, sec..19.
14. Albert C.Leighton, “Secret Communication among the Greeks and Romans,” Technology and Culture 10, no. 2 (April 1969): 139–54, p. 154 cited here. Leighton’s citation for the letter was Ausonius’ Epistles, 28.
15. Leighton, “Secret Communication,” 153, footnote 61, cited here.

16. A dissenting view is offered by Henry R.Immerwahr in Attic Script, A Survey (New York: Oxford University Press, 1990). On p. 15, he wrote, “Before the time of Draco Athens was a cultural backwater — not a suitable location for the composition of the Homeric poems, as some have thought.” And on p. 20 he wrote, “Corinth clearly took the lead in the custom of applying in-scriptions to vases.” He views the work in Athens as imitative of the work in Corinth.

17. Immerwahr, Attic Script, 45.

18. John Boardman, Athenian Black Figure Vases (New York: Oxford University Press, 1974), 201.

19. Dan Vergano, “Amazon Warriors’ Names Revealed Amid ‘Gibberish’ on Ancient Greek Vases,” National Geographic (September 22, 2014), http://news.nationalgeographic.com /news/2014/09/140923-amazon-greek-vase-translations-science/.

20. Umberto Eco, Foucault’s Pendulum, trans. William Weaver (San Diego, New York, London: Har-court Brace Jovanovich, 1989), 24.

21. “Bamf”“Snikt”是美国漫画中常出现的两个拟声词，谢尔顿认为这两个词的读音和印度的语言或者拉杰什的口音有类似之处，故他认为拉杰什在理解这两个词的时候会遇到困难。——译者注

22. Big Bang Theory transcripts, https://bigbangtrans.wordpress.com/series-4-episode-09-the -boyfriend-complexity/.

23. Adrienne Mayor, John Colarusso, and David Saunders, “Making Sense of Nonsense Inscriptions Associated with Amazons and Scythians on Athenian Vases,” Hesperia: The Journal of the American School of Classical Studies at Athens 83, no. 3 (July–September 2014): 447–93, p. 466 cited here.

24. Adrienne Mayor, John Colarusso, and David Saunders, “Making Sense of Nonsense Inscriptions Associated with Amazons and Scythians on Athenian Vases,” Hesperia: The Journal of the Amer-ican School of Classical Studies at Athens 83, no. 3 (July–September 2014): 447–93, pp..486–87 cited here.

25. Dan Vergano, “Amazon Warriors’ Names Revealed Amid ‘Gibberish’ on Ancient Greek Vases,” National Geographic, September 22, 2014.

26. Adrienne Mayor, The Amazons: Lives and Legends of Warrior Women across the Ancient World (Princeton, NJ: Princeton University Press, 2014), 11.

27. 因为不知道这些艺术家的具体姓名，研究者只能用这些假名来指代他们。——译者注

28. E-mail from Adrienne Mayor to the author, received June 25, 2015.

29. Adrienne Mayor, John Colarusso, and David Saunders, “Making Sense of Nonsense

Inscriptions Associated with Amazons and Scythians on Athenian Vases," Version 2.0, Princeton/Stanford Working Papers in Classics, July 2012, 27–28.

30. E-mail from Adrienne Mayor to the author, received June 25, 2015.

31. E-mail from Adrienne Mayor to the author, received June 25, 2015.

32. Adrienne Mayor, John Colarusso, and David Saunders, "Making Sense of Nonsense Inscriptions Associated with Amazons and Scythians on Athenian Vases," Hesperia: The Journal of the Amer-ican School of Classical Studies at Athens 83, no. 3 (July–September 2014): 447–93, p. 489 cited here.

33. Adrienne Mayor, John Colarusso, and David Saunders, "Making Sense of Nonsense Inscriptions As-sociated with Amazons and Scythians on Athenian Vases," Hesperia: The Journal of the American School of Classical Studies at Athens 83, no. 3 (July–September 2014): 447–93, p. 465 cited here.

34. E-mail from David Saunders to the author, received June 26, 2015.

35. Ole Franksen, Mr. Babbage's Secret: The Tale of a Cypher and APL (Englewood Cliffs, NJ: Prentice-Hall, 1985), 86.

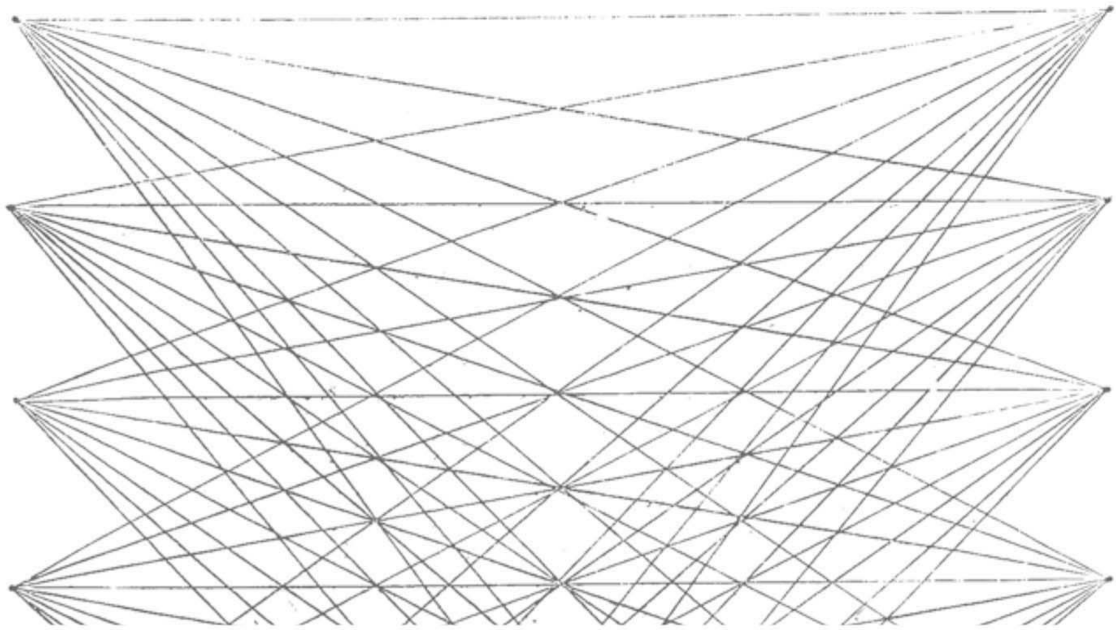
36. Stig Eliasson, "When 'Chance' Explanations Turn Tenuous: Basque Verbal Morphology, Argu-ment Marking, and an Allegedly Nonsensical Danish Runic Inscription."

37. Eliasson, "When 'Chance' Explanations Turn Tenuous."

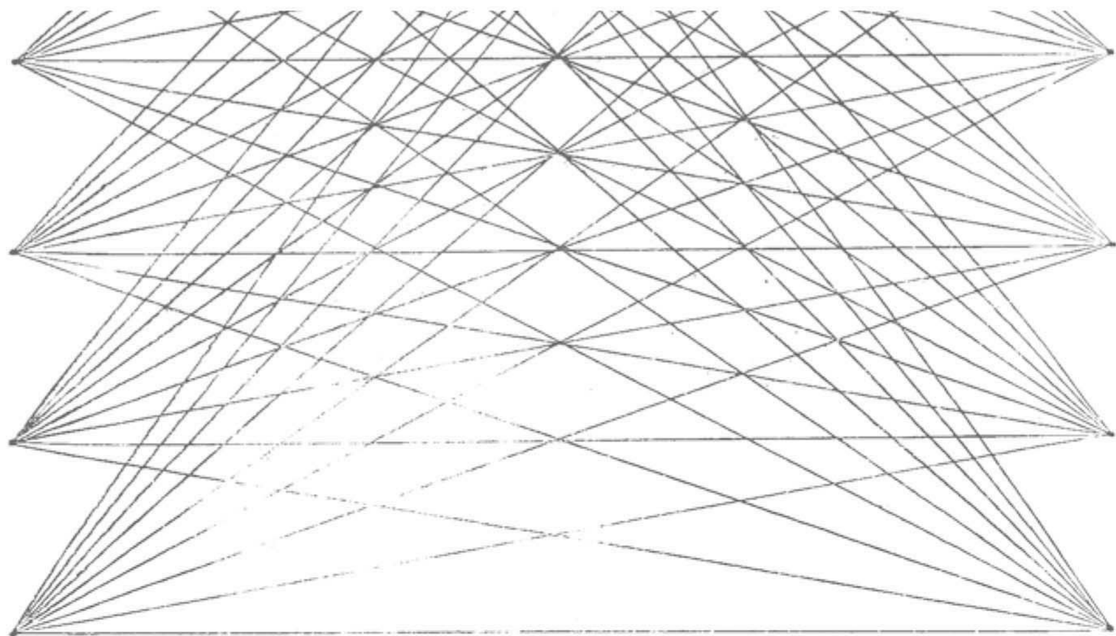
38. Michael P.Barnes, Runes: A Handbook (Suffolk, U.K.: Boydell Press, 2012), 167.

39. Barnes, Runes, 202.

40. Barnes, Runes, 24.



第3章
多拉贝拉密码



从上一章中我们可以看出，很多古代密码只用了一些简单的加密系统。某些古代密码之所以一直未被破解，可能仅仅是因为人们没有意识到这些文字是密码。对于现代的破译者而言，要想破译密码，首先需要做的就是判断这些密码究竟是以何种语言写成的。这重语言判断上的困难为古代密码的破解增加了难度。那么，如果一段简单的密码产生于现代，并且是用英语写成的，这样的密码是否还可能长期无法被破译呢？这个问题的答案是肯定的，一位英国作曲家就为我们提供了这样一个例子。

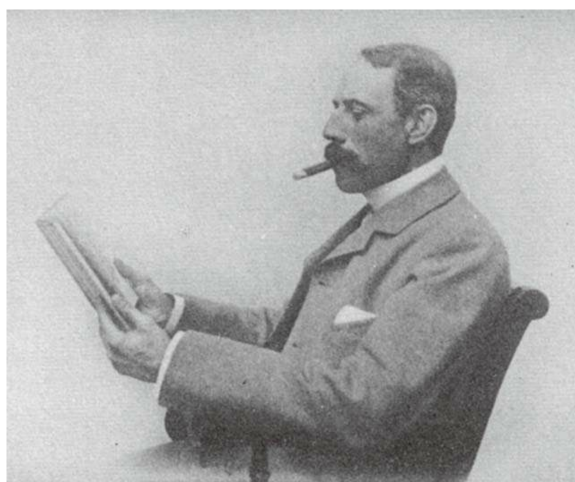


图3-1 爱德华·埃尔加 (1857—1934)

爱德华·埃尔加最著名的音乐作品是《威仪堂堂进行曲》（*Pomp and Circumstance*）(注)，这首曲子已经成为美国高中毕业典礼的必奏曲目。此外，他还创作过《谜语变奏曲》（*Enigma Variations*）等著名曲目。在《谜语变奏曲》中，埃尔加用14段不同的变奏分别代表他的14位朋友和家庭成员。此外，《谜语变奏曲》中还有一个隐藏的主题，埃尔加从未透露过这个主题是什么。对于认识埃尔加的朋友和家人而言，他们可以自行猜测不同的变奏对应的是什么人，以及这些变奏象征的究竟是怎样的意象——相信这一定是一项十分有趣的娱乐活动。

比如，《谜语变奏曲》的第一段变奏（速度标记为*L'istesso tempo*，意为“相同速度”）“C.A.E.”代表的是他的妻子卡罗琳·艾丽斯·埃尔加（Caroline Alice Elgar）。埃尔加用4个音符来代表卡罗琳，因为他每次回家时都会用口哨向卡罗琳吹这4个音符。

其他主题与人物之间的联系相对不是很紧密。埃尔加解释过，第十一段变奏（速度标记为*Allegro di molto*，意为“极快板”）“G.R.S.”代表的

是赫里福德大教堂的管风琴师乔治·罗伯逊·辛克莱（George Robertson Sinclair）。

> 然而，这段变奏与管风琴或者教堂没有任何关系，甚至与乔治·罗伯逊·辛克莱的联系也不够紧密。一开始几个小节表现的是乔治的牛头犬丹（Dan，一个为人熟知的角色）从陡峭的河岸掉进了瓦伊河里（第一小节）。然后，丹游到上游，并找到了一个可以爬上岸的地方（第二小节和第三小节）。在上岸的时候，丹发出了高兴的吠叫声（第五小节的后半段）。辛克莱对我说："把这些写成音乐吧。"我听从了他的建议，写出了这段变奏。(注)

《谜语变奏曲》的另一段变奏代表的是埃尔加妻子的一位挚友的女儿。在创作这段音乐的时候，这位姑娘的名字（她出嫁前的闺名）叫作多拉·彭尼，而埃尔加称她为"多拉贝拉"。"多拉贝拉"这个名字来自莫扎特的歌剧《女人心》（*Così fan tutte*）。许多认识多拉的人都认为关于她的这段变奏非常美妙。



图3-2 多拉•彭尼
(Dora Penny，1874—1964)

现在，我们要谈到这段至今未被破译的多拉贝拉密码了。这段密码出现于埃尔加写给多拉的一封信中，落款日期为1897年7月14日。甚至连多拉本人也无法破译这段文字的意义。图3–3为从这封信中摘录的密码部分。

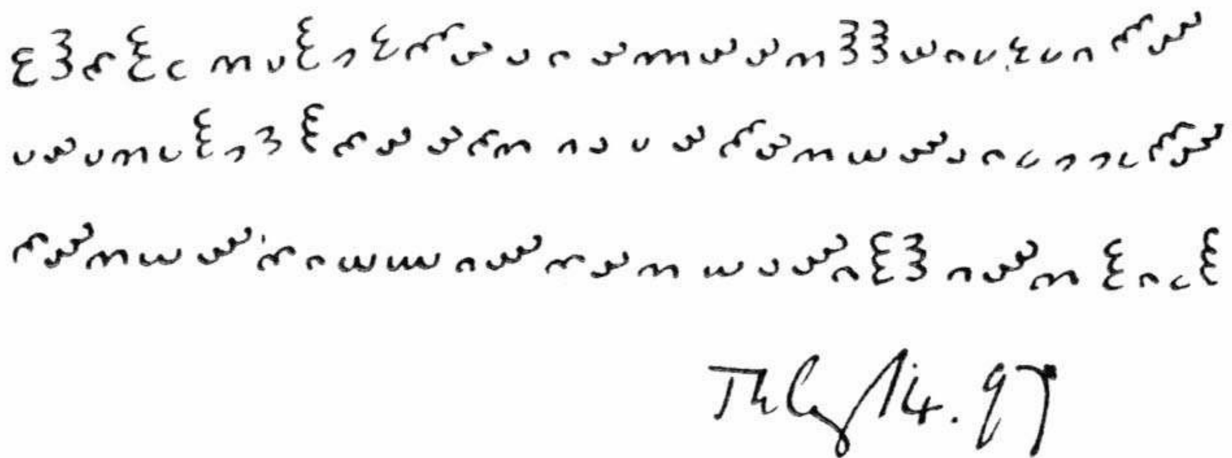


图3-3 多拉贝拉密码，得名于埃尔加对收信人多拉·彭尼的昵称“多拉贝拉”

埃尔加为什么会想到用这些弯弯曲曲的线条来代表字母呢？如果我们看一下埃尔加签名时所用的首字母缩写，也许就能找到这个问题的答案。

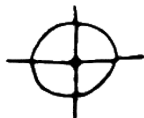


图3-4 埃尔加签名时所用的姓名首字母缩写

埃尔加会不会是在写自己的姓名首字母缩写时想到了可以用这些弯弯曲曲的线条来代表文字呢？那些看起来像是字母E和字母W的图形是否真的代表字母E和字母W呢？由于埃尔加从未解释过他使用的这些密码符号的最初来源，所以对这些问题我们只能进行猜测。

虽然这段密码用弯弯曲曲的线条代替了字母，但是它看起来非常简单。这段密码似乎是一段删除了空格的单套字母替代式密码（MASC密码）。然而，在使用了所有破译MASC密码的技巧之后，都未能从这段密码中破解出任何有意义的内容。接下来我将向读者介绍一些研究者尝试提出的各种解法，然而在这些解法中，没有一种获得过广泛的承认。

对解法的不断探寻



1970年，埃里克·萨姆斯（Erik Sams）提出了多拉贝拉密码的一种可能解法。萨姆斯称自己曾在战争期间有过破译密码的经验，但却没有给出更多这方面的细节。但是，对于他的生平，我们还是收集到了一些零散的信息。萨姆斯曾获得过剑桥大学圣体学院的奖学金，当时他只有16岁。然而，他并没有接受剑桥大学的录取，而是在17岁的时候加入了军方的情报机构。若干年以后，当已经没有继续保密的必要时，萨姆斯才向公众谈起了情报机构的面试过程。

> 面试官会问面试者若干问题，其中一个问题是："你会下棋吗？"恐怕大家也能够猜到，第二个问题是："你喜欢填字游戏吗？你擅长玩填字游戏吗？"但是，第三个问题却是："你喜欢音乐吗？你能看得懂乐谱吗？"当时我就意识到，对音乐的兴趣和对密码的兴趣之间有着很清楚的联系，我至今仍然相信这一点。这其中的一个原因是（如果这一点有价值的话），不管作曲家是否对密码有兴趣，一代又一代的作曲家都把音乐看作一种交流的形式，更具体来说，是一种秘密的语言，只有明白这种语言的人才能够读懂它。人们经常用这种方式来看待音乐。此外，我还认为，音乐和密码之间在结构上非常相似。[注]

关于萨姆斯的工作的具体性质，一位名叫罗恩·罗森鲍姆（Ron Rosenbaum）的作者从萨姆斯那里得到了一些详细的信息。

> 萨姆斯告诉我，在第二次世界大战期间，他是一名密码专家。他的工作地点是传奇的布莱奇利园密码破译站，也就是破解恩尼格

玛密码机的地方。萨姆斯声称，在布莱奇利园工作的时候，他所在的团队，代号为“魔术（MAGIC）”，曾经破解过日本的密码系统。注

另外一个来源则称，萨姆斯不仅破解过日本的密码系统，还破解过德国的密码系统。

在成为专业的密码破译员之前，萨姆斯就已经对密码学产生了兴趣。1947年，他离开军队以后，也仍然保持着对破译密码的兴趣。在之后的一次采访中，萨姆斯这样描述自己对密码破译的热情：

我的第一份工作是战争时期英国陆军情报机构的密码破译工作。我终生保持着对密码的兴趣。我的意思是说，这是一种我在孩提时代就有的热情，我喜欢暗号和密码一类的东西。我在音乐中也能看到暗号和密码。事实上，如果把世界想象成一个巨大的档案收藏馆的话，世界上的所有档案中都存在大量的密码和暗号，这其中的许多秘密仍然尚未解开，许多速记简写的方式是人们看不懂的，许多暗号和密码是人们无法理解的。关于英国内战、美国南北战争、美国独立战争的记录，各种速记式的日记（比如佩皮斯日记、克伦威尔的秘书的日记、威廉姆·克拉克的日记）等，都没有被读懂，而且实质上是没有办法被读懂的。注

1947年，萨姆斯离开了军队。1950年，他获得了剑桥大学的法语和德语学士学位。就像许多曾经试图破译伏尼契手稿的人一样，以萨姆斯的能力和背景，对付这套密码似乎绰绰有余。然而，对于多拉贝拉密码，萨姆斯的解答是这样的：

STARTS: LARKS! IT’S CHAOTIC, BUT A CLOAK OBSCURES MY NEW LETTERS, A, B （alpha, beta, i.e. Greek letters or alphabet）

BELOW：I OWN THE DARK MAKES E.E.SIGH WHEN YOU ARE TOO LONG GONE.

［开始：云雀！一切都很混乱，但是一个斗篷遮住了我的新字母——A、B（希腊字母α、β或字母表）

下方：当你已离去太久，我承认黑暗使E. E. 叹息。］

虽然埃尔加是一位著名的作曲家，而不是著名作家，但是我们很难想象他会写出一段如此杂乱和不连贯的话。

另一种可能的解法是由琼·帕尔默（Jean Palmer）提出的，她是《暗号与密码答读者问专栏》（*The Agony Column Codes & Ciphers*）一书的作者。《暗号与密码答读者问专栏》一书中包含了1 000多种发表在英国报纸个人专栏中的密码，其中大部分来自维多利亚时代的报纸。维多利亚时代的人们认为，在报纸专栏上用密码登载消息是一种安全的秘密交流的方式！在书的最后，作者提出了对这些密码的解答，但并不是每一条加密信息都被破译出来了。书中的许多密码并没有被解开。虽然这本书中的密码非常有趣，但是由于篇幅的限制，在这里我没有办法与读者详细讨论这些密码。

在用1 000多条登在报纸上的密码进行“热身”以后，帕尔默在2007年注提出了对多拉贝拉密码的解法，初始解答如下：

BLTACEIARWUNISNFNNELLHSYWYDUO

INIEYARQATNNTEDMINUNEHOMSYRRYUO

TOEHO’TSHGDOTNEHMOSALDOEADYA

这样的结果实在太令人失望了！我们没有办法在这段字母中加入空格以得到一段能够读懂的英文。帕尔默解释说，接下来的步骤是“把其中的倒读隐语反过来”。在完成了这个步骤，并且在单词之间加入空格

以后，帕尔默得到了以下结果：

B LCAT IE AWR USIN NF NN ESHLL WY YOUD

INTAQRAYEIN NET DMINUNEHO M SRRY YOU

THEO O ’ THS GOD THEN M SO LA OD E ADYA

接下来的一个步骤是“改正根据音标拼写的单词，并对一些微小的错误进行修正（此时若干符号的方向尚不清楚）”。在完成了这一步以后，帕尔默得到了如下的结果：

B（Bella）hellcat i.e. war using ?? hens shells is why your

antiquarian net diminishes hem sorry you

theo oh ‘tis God then me so la do E（Elgar）Adieu

这段不通顺的话大概译文如下：

B（贝拉）巫婆，也就是战争使用？？母鸡贝壳因此你

古董网减少褶边对不起你

神哦上帝然后我嗦啦哆E（埃尔加）再会

这一结果看起来仍然极其不自然。事实上，这种解法的提出者的名字背后还藏着另外一重密码。我发现“琼·帕尔默”并不是一个真实的人名，而是托尼·加夫尼（Tony Gaffney）使用的一个假名。我写信给托尼·加夫尼进行求证，以下是他的回复：

是的。这源于我的幽默——这是一个字母顺序重排的字谜。要是我解开了所有密码（指《暗号与密码答读者问专栏》一书中的1000多种密码），那么我就会将“夏洛克·福尔摩斯”的字母重排作为假名。㊟

在之前的章节中，我们已经解释过，所谓“字母顺序重排的字谜”就是对一个姓名、一个单词，或者一组单词中的原始字母顺序进行重排，得到的新词句仍然有意义。有些“字母顺序重排的字谜”是很滑稽的，比如DORMITORY（宿舍）= DIRTY ROOM（脏房间）。下面这些字谜我留给读者自己去解：

1. 你能否重排“ROAST MULES”得到一个英文单词？这个字谜来自艾拉·莱文（Ira Levin）的小说《罗斯玛丽的儿子》（Son of Rosemary）。

2. 你能否改变“MR. MOJO RISIN”的字母顺序，得出一个著名音乐家的名字？

3. 你能否改变“THE MORSE CODE（莫尔斯电码）”的字母顺序得到另外3个英文单词，并且保证它们和莫尔斯电码相关？

4. 你能否通过重排字母顺序把“PUNCH EVILDOERS”变成两个完全不同的单词？

5. 你能否找出“JEAN PALMER”背后隐藏的名字是什么？

6. 你能否改变“I CARRY NO LAST END HOUR”的字母顺序得到一个著名作家的名字？㊟

如果读者想要自己设计一些字母顺序重排的字谜的话，以下这个网站能够给你提供一些帮助：http://www.ssynth.co.uk/~gay/anagram.html。

2007年，为了庆祝埃尔加150周年诞辰，埃尔加协会设置了一笔1

500英镑的奖金。任何人只要能找到多拉贝拉密码的正确解法，就可以获得这笔奖金。奖金设立以后，埃尔加协会收到了许多研究者提交的各种解法，包括上文已经介绍过的托尼·加夫尼的解法，但是所有这些解法都没有被接受。

2009年，蒂姆·S.罗伯茨（Tim S.Roberts）提交了多拉贝拉密码的又一种解法。罗伯茨是澳大利亚中央昆士兰大学的一名讲师，(注)他的解法如下：

P.S. Now droop beige weeds set in it — pure idiocy — one entire bed! Luigi Ccibunud luv'ngly tuned liuto studo two.

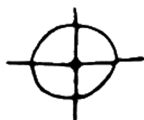
（又及：现在让中间的米色野草下垂——完全是白痴——整整一床！路易吉·西邦纳德慈爱地给琉特琴调音，学习2。）

虽然这段破译出来的明文看起来还是很奇怪，但是罗伯茨在做替换的时候已经将文中一些不自然的地方做了修正了。比如，罗伯茨一开始得到的词是“drocp”，他把这个词改成了“droop”，因为他认为这个词中的c是拼写错误。还有，以上明文中的“pure”一词原来是“bure”。

至于这段修正过后的明文究竟是什么意思，罗伯茨给出了一种解释，然而，事实上正确的解法很少需要附加额外的解释。当密码破译者声称密码中包含“多层加密”的时候，这通常都意味着他们给出的解答根本就是错误的。

在假设这段密码是MASC密码的前提下，各路研究者给出了以上这些最好的解答。由于上述这些解法实在缺乏说服力，所以也许这段密码所使用的是某种比MASC密码更加复杂的加密方式。为了了解埃尔加可能使用哪些其他加密方式，下面我们来研究一下埃尔加与密码的各种已知的联系。

埃尔加的第一个广为人知的密码
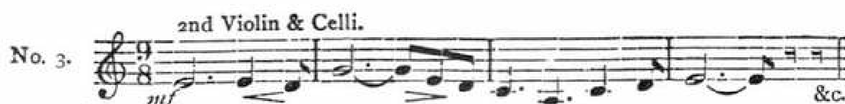


现在，让我们把时钟往回拨，回到埃尔加创作出他的第一条广为人知的密码的时间，此时距离多拉贝拉密码的创作大约还有10年。图3–5中展示了这段密码。

可以看到，埃尔加把这段密码写在一张音乐会节目单的边缘空白处。由于这段音乐的作曲者是李斯特，所以这张纸通常被称为“李斯特碎片”。在图3–6中，我把埃尔加的这段密码放大，以便读者能够更清楚地看到密码的内容。

专门研究埃尔加的专家杰罗尔德·诺思拉普·穆尔（Jerrold Northrup Moore）给出了这段密码的一种解法，该解法是由安东尼·索利（Anthony Thorley）提出的。

> 1866年4月10日，他去水晶宫参加了一场庆祝弗朗茨·李斯特75岁诞辰的音乐会。这是多年来李斯特再次访问英格兰，指挥家曼斯所带领的交响乐团也超越了自己。这位老神父（指李斯特）不仅和曼斯握了手，还多次向鼓掌欢呼的听众们鞠躬致意。爱德华把他自己对当晚音乐的评价用铅笔以一段密码的形式写在了演出节目单上。从这段密码中，我们可以看出埃尔加早就对这种神秘艺术展现出了兴趣，这种神秘的艺术比双关语更能隐藏秘密，并且能够展示出创作者独特的聪明之处。很多年以后，这段关于李斯特音乐的密码被破译如下：“GETS YOU TO JOY, AND HYSTERIOUS.（给你带来快乐，也让你诡秘。）”（这种解法是由安东尼·索利于1977年提出的。）“HYSTERIOUS”是一个合成词，前半段来自“hysteria”（歇斯底里），后半段来自“mysterious”（神秘的）。注

This is followed by :—



—leading eventually to the "second subject" :—
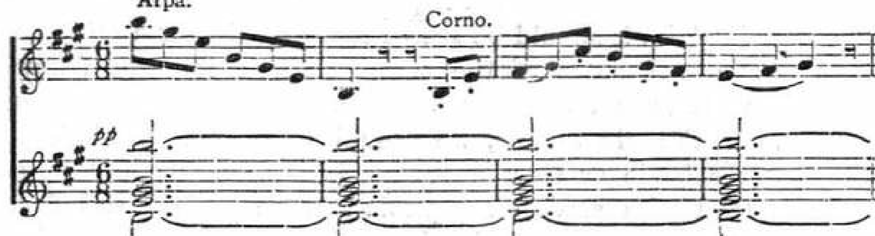


The "working out" section, commencing :—



—is chiefly occupied with the development of the "first subject," freely treated. To this succeeds an independent episode :—

No 6. *Allegretto pastorale.*



—which is subsequently heard in combination with the "second subject."

An *Allegro marziale*, evolved from the two principal subjects, and commencing thus :—

No. 7. *Animato.*



—brings the work—after a return to No. 2—to a brilliant and triumphant end.

[C. A. B.]

图3-5 埃尔加早期创造的一段密码

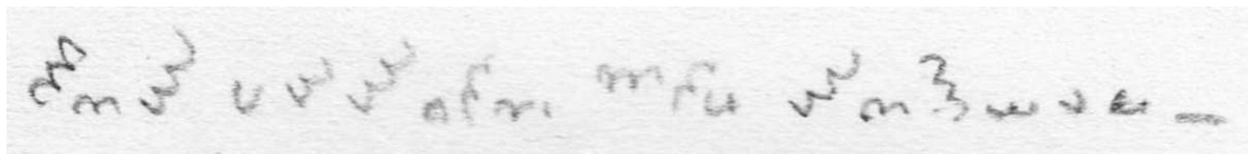


图3-6 “李斯特碎片”的放大图

然而，这种解法根本就不合理！从下面的图3–7中读者不难看出，不仅同样的弯曲图形对应于不同的字母，而且弯曲图形的总数目也与解答中的字母总数不相符。这一解答的最后6个字母根本无法与任何密文中的图形相对应。

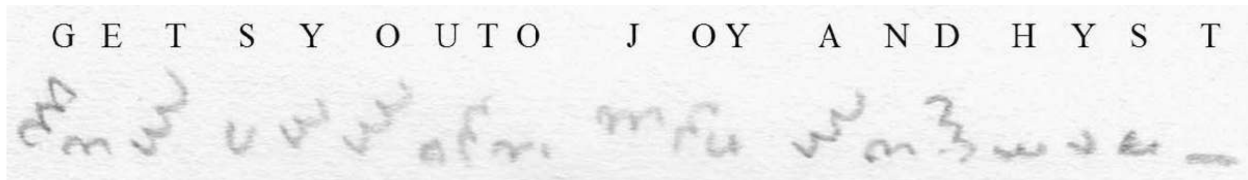
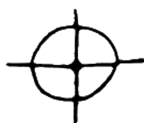


图3-7 对研究者提出的一种解法进行验证

当然，其他研究者还提出过“李斯特碎片”等其他一些解法。虽然这些解法的字母数目与密文中的弯曲图形数目一致，但它们的意义也不太合理。因此，这段“李斯特碎片”密码似乎也应该被视为一段尚未破解的密码，也就是说，这段密码并不能像我们希望的那样对多拉贝拉密码的破译工作提供太大的帮助！接下来，我们再把时钟向后拨，来研究一下埃尔加的最后一个广为人知的密码。

埃尔加的最后一个密码



埃尔加留下了一本20世纪20年代的笔记本，在这个笔记本的若干页中，出现了同样用这种奇怪的弯曲图形写成的另外一段密码，这段密码的创作时间比多拉贝拉密码晚得多。由于埃尔加在这个笔记本中给出了这段密码的密钥，所以读者可以自行破解这段弯曲的图形。在下幅图之后，我将给出这段密码的部分明文信息。

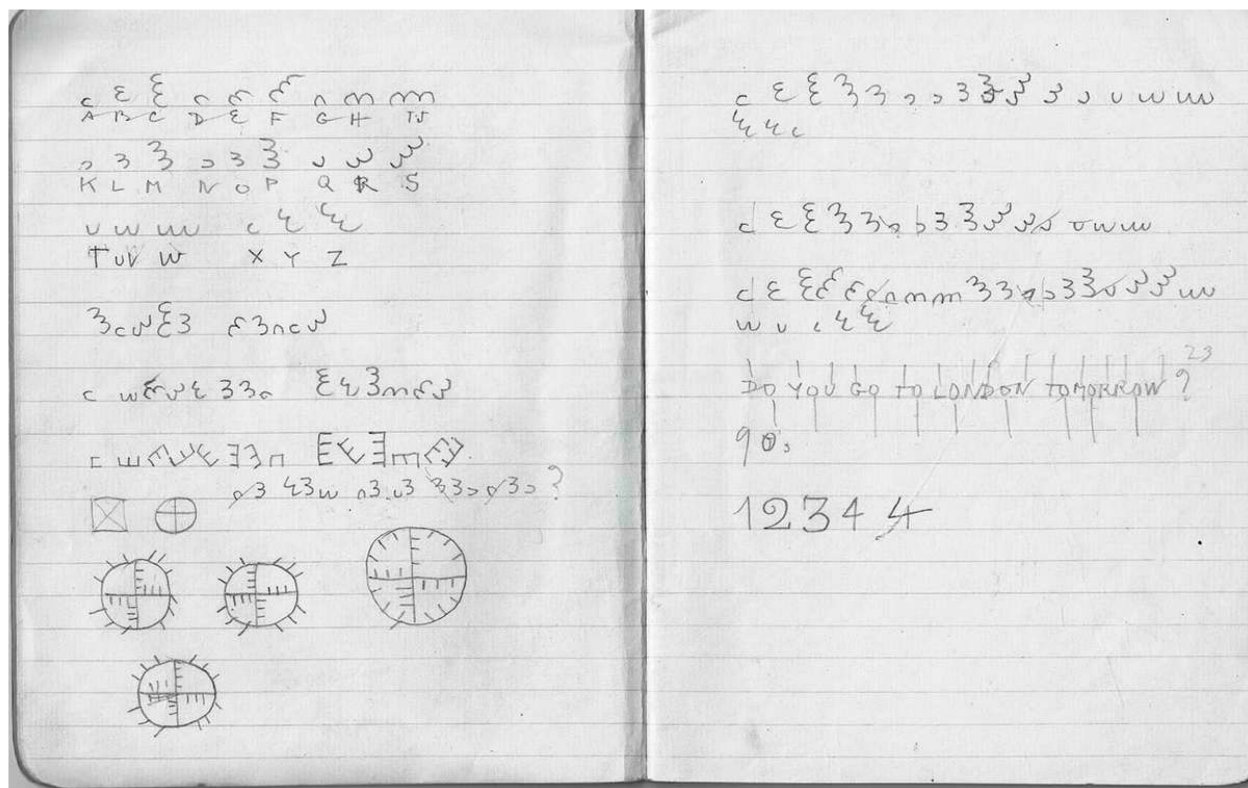


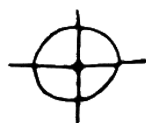
图3-8 埃尔加写的另一些加密文字

在左页的顶部，埃尔加给出了密码的替换字母表。注意I和J这两个字母都是用同一个弯曲符号来表示的，U和V也是用同一个弯曲符号来表示的。我们可以用这套替换字母表破解出这个笔记本中的这段密码，但是，把这套替换字母表代入多拉贝拉密码或者李斯特碎片密码后，却只能得到一些毫无意义的文字。

如果我们把这套替换字母表代入笔记本上的这段密码中，我们就会得到“马可·埃尔加”（Marco　Elgar）这个名字。“马可·埃尔加”并不是爱德华·埃尔加的某位亲戚，而是他的宠物——一只长毛垂耳狗的名字。埃尔加非常喜欢狗，至少，他非常喜爱他这只宠物狗。

因此，“李斯特碎片”（尚未破解）并不能帮助我们破译多拉贝拉密码，这个笔记本上的密码（已破解）也不能。除了以上两段密码以外，还有另外一份文件上也包含埃尔加潦草的手写字迹。这份文件的日期比本段中讨论的这个笔记本要更早，它是埃尔加为破译他人创造的密码时留下的资料。

来自斯库林的挑战



1896年，约翰·霍尔特·斯库林（John Holt Schooling）为《蓓尔美尔杂志》（*The Pall Mall Magazine*）撰写了一系列关于密码学的文章，从1月刊开始，每月发表一篇，一共发表了四篇。在这一系列文章中，他按照时间顺序向读者介绍了密码学历史。此外，在每篇文章的结尾处，斯库林还会留下一个密码来让读者破译。在第四篇文章中，他向读者介绍了一种叫作“无政府主义密码”的密码。这种密码之所以被称为“无政府主义密码”，是因为19世纪时反对沙皇的无政府主义者曾使用这种密码，并且这种密码有可能就是由这群人发明的。“无政府主义密码”并不复杂，但是要解开它也需要经过一系列的步骤。斯库林向读者提供了图3–9中的这个表格，通过这个表格就可以把原始信息中的字母转化成数字。上述的转化原理和我们在第2章中提到的波利比奥斯密码的原理类似。这是“无政府主义密码”加密过程的第一步。

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	X
5	V	W	X	Y	Z

图3-9 用于把字母转化为数字的表格

请注意，在斯库林提供的上述表格中，字母X出现了两次——这是一个笔误，第一个字母X应写作字母U。此外，在这个网格中，我们找不到字母J的身影，这是密码设计者有意为之的，因为一个5×5的网格只能容纳25个字母。有时候我们必须有所取舍！

加密的第一步很简单：对于任何一个字母，你只需要在上述表格中找到这个字母所在的横行数和纵列数。比如，字母M出现在上述网格的第3行第2列，我们就用数字32来表示。斯库林举例所用的明文信息是“MEET ME IN PARIS ON MONDAY（我们星期一在巴黎见面）”。首先，他把这个句子中的每一个字母与上述网格中的横行数和纵列数对应起来，这一步的结果参见图3–10的第一行和第二行。这幅图来自斯库林的文章。下图的第二行是一个MASC密码。但是，为了让这段密码更难破解，我们在第二行的数字下面再写上一个关键词。在斯库林给出的例子中，这个关键词是“TYRANT（暴君）”。因为关键词的长

度远小于整条信息的长度，因此我们必须把这个关键词重复书写多次。

① M E E T M E I N P A R I S O N M O N D A Y

② 32·15·15·44·32·15·24·33·35·11·42·24·43·34·33·32·34·33·14·11·54

③ T Y R A N T T Y R A N T T Y R A N T T Y R

④ 44·54·42·11·33·44·44·54·42·11·33·44·44·54·42·11·33·44·44·54·42

⑤ 76·69·57·55·65·59·68·87·77·22·75·68·87·88·75·43·67·77·58·65·96

图3-10 以“TYRANT”为关键词的一段样本密码

在关键词行（第三行）下面，我们把这些关键词按照上述网格的规则转化成数字，这样就得到了图中的第四行。在加密的最后一个步骤中，我们把第二行的数字和第四行的数字加起来的，得到最终的密文，也就是图中的第五行。

注意，虽然原始明文信息中出现了三次字母E，但是这三个字母E却被加密成了三个不同的数值，分别是69、57，以及59，这是因为每一个字母E对应于关键词“TYRANT”中不同的字母。有时，明文信息中相同的字母也可能对应于关键词中同样的字母，比如，上述明文信息中的字母I就出现了这样的情况。但是，用这种方法加密后，同一个字母确实**有可能**会被加密成不同的数值。这种加密系统被称为“多套字母替代式密码”，因为同一个字母可以被不同的符号替代，而在“单套字母替代式密码”（MASC密码）中，同一个字母只能被同一个符号所替代。第一次见到“多套字母替代式密码”的人常常会觉得这种加密系统很难破解，前文提到的各种破解MASC密码的技巧也都无法破译它。显然，斯库林也认为这是一种非常好的加密方式。

在第四篇文章中，同前三篇文章一样，斯库林也留了一道密码题让读者破解。这次的挑战参见图3–11。

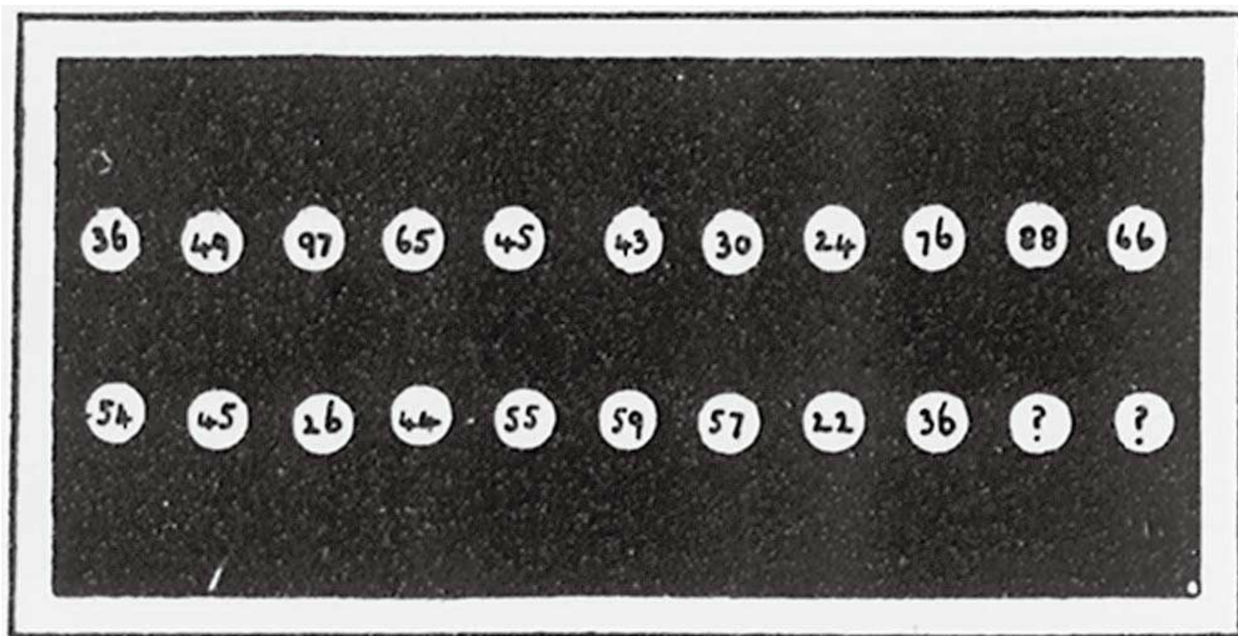


图3-11 斯库林在最后一篇文章中留给读者的挑战

斯库林告诉读者，这个待解决的密码和文章中举出的例子十分相似，然而他又表示：

> 但是，文末这段密码中所使用的关键词却并不是例子中所使用的“TYRANT”一词，因此没有任何人能够破解接下来的这个密码。虽然“魔盒”已被打开，让我们看到了过去若干个世纪中密码的秘密，但这个“魔盒”却又一次在我们面前紧紧地关上了。在未来的100年中，再也不会有人能打开这个“魔盒”的封条。[注]

虽然斯库林的上述警告听起来十分吓人，但埃尔加并没有被吓倒。埃尔加不仅开始着手破译这段密码，并且最终取得了成功。在埃尔加出生的英国伍斯特郡博物馆中收藏了一系列卡片，从这些卡片上，我们可以看到埃尔加是如何解开斯库林的这段密码的。接下来，让我们来逐张检视这些卡片上的内容，以便理解埃尔加破译这段密码的方法和步骤。在破译出斯库林的这段密码后不久，埃尔加便创造出了著名的多拉贝拉密码，或许两段密码间存在一定联系。

第1张卡片上并没有什么特别的内容，这张卡片只是简单地列出了密码的密文。

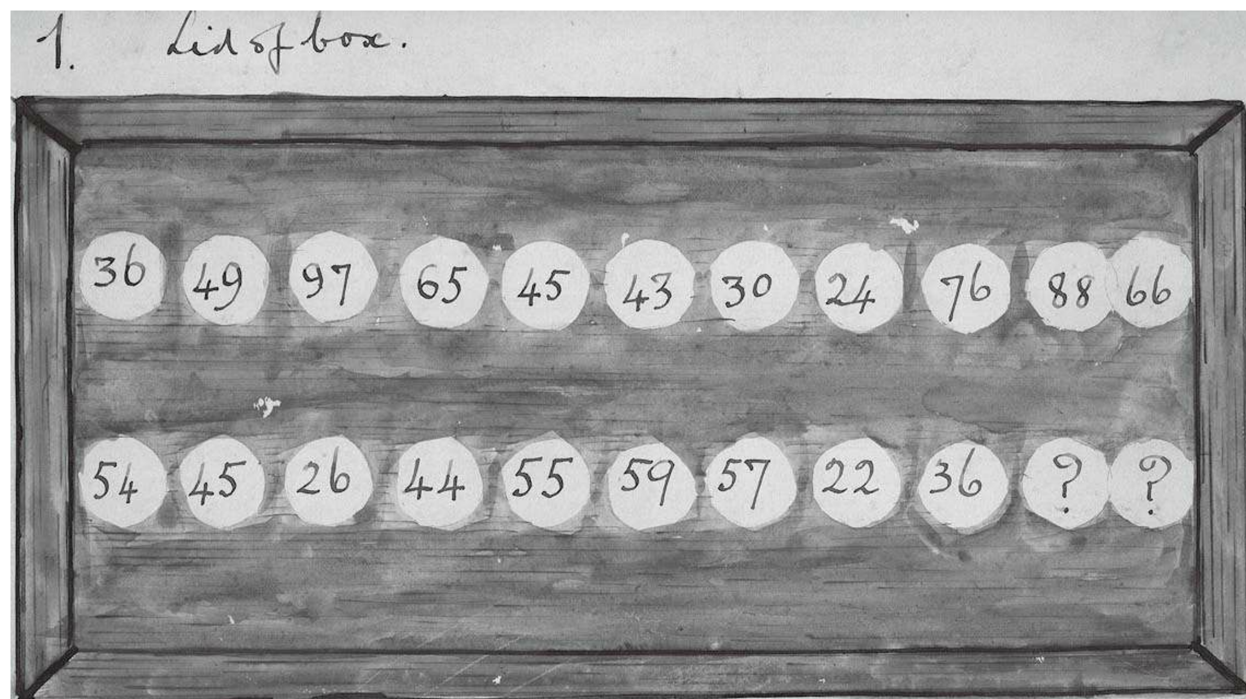


图3-12 第1张卡片：埃尔加给出了这段密码，并将这段密码标记为“盒盖”

第2张卡片上列出了能将原始信息和关键词转化成两位数字的网格。埃尔加修正了斯库林原始表格中字母X出现了两次的错误。

在第3张卡片上，埃尔加提供了一个用这种方法加密的例子。这张卡片上特别强调了一个重点，即同一个字母有时可以被加密成不同的数值。埃尔加写道：“任何语言中的任何一个单词都可能是这段密码的关键词。”由于当时还没有计算机，埃尔加没有办法用计算机通过穷举法尝试所有可能的关键词。

在第4张卡片上，埃尔加又提供了另外一个例子。埃尔加指出，在第一个步骤完成以后（即将原始信息转化成数字后），所得到的结果是“非常容易破译的”。为了说明这一点，埃尔加列出了一些样本字母出现的概率（样本中，代表字母E的15出现了10次）。“无政府主义密码”之所以比MASC密码难破译，是因为增加了关键词这个步骤。

图3-14 第3张卡片：用一个例子解释这段密码的原理

图3-13 第2张卡片：把字母转化为数字的表格

在第5张卡片上，埃尔加解释了知道关键词的收信人可以通过怎样的步骤把密文翻译成原始信息。

在第6张卡片上，埃尔加终于开始回归正题，也就是开始破译斯库林的密码了。埃尔加注意到，密文中的倒数第二个数字是22。产生22这个数字的唯一可能性是：密文字母和关键词字母都对应于数字11。也就是说，明文信息和关键词中的字母都是A。这两个字母对应的数值（11）加在一起就是22。通过这个巧妙的观察，埃尔加迅速解出了一个明文中的字母和一个关键词中的字母！

图3-15 第4张卡片："无政府主义密码"与容易破译的MASC密码的比较

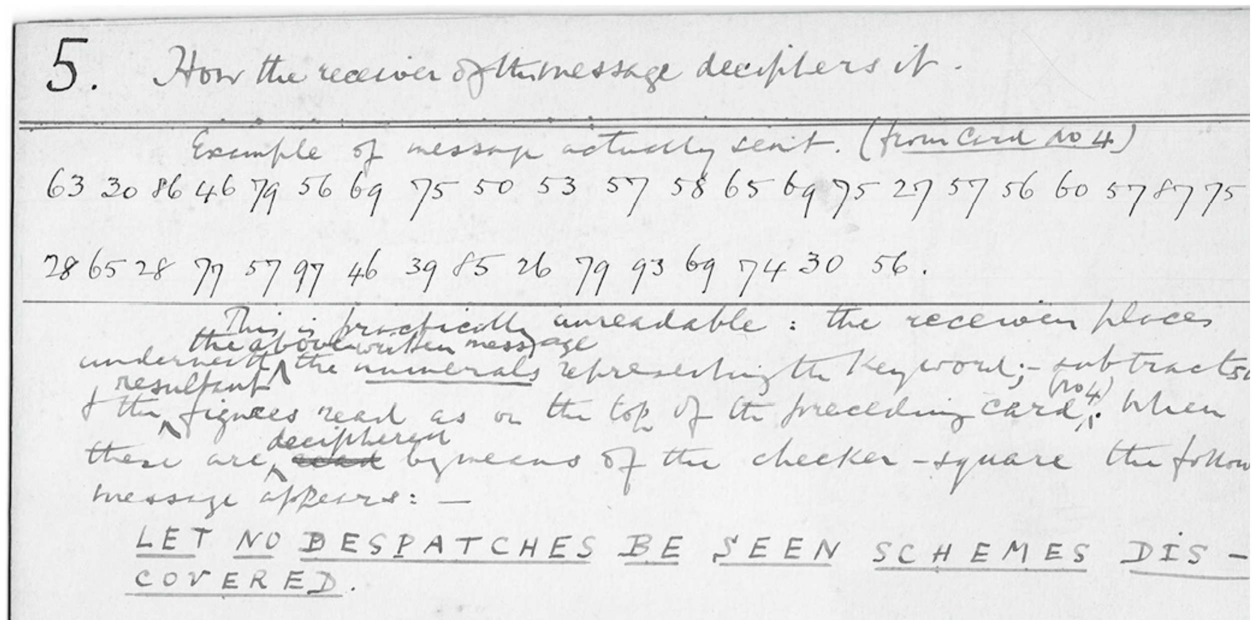


图3-16 第5张卡片：解释收信人如何利用关键词把密文翻译成原始信息

接着，埃尔加又注意到密文中的30这个数字。30也只可能由一种方式获得：那就是15 + 15 = 30。也就是说，此处明文和关键词中的字母都是E。当然，从数学上来看，还可以通过其他方式得到30这个数字，比如14 + 16 = 30。但是，上述将字母转化为数字的网格没有16这个数值，因此这种可能性可以排除。埃尔加把得到的数值继续填写出来。

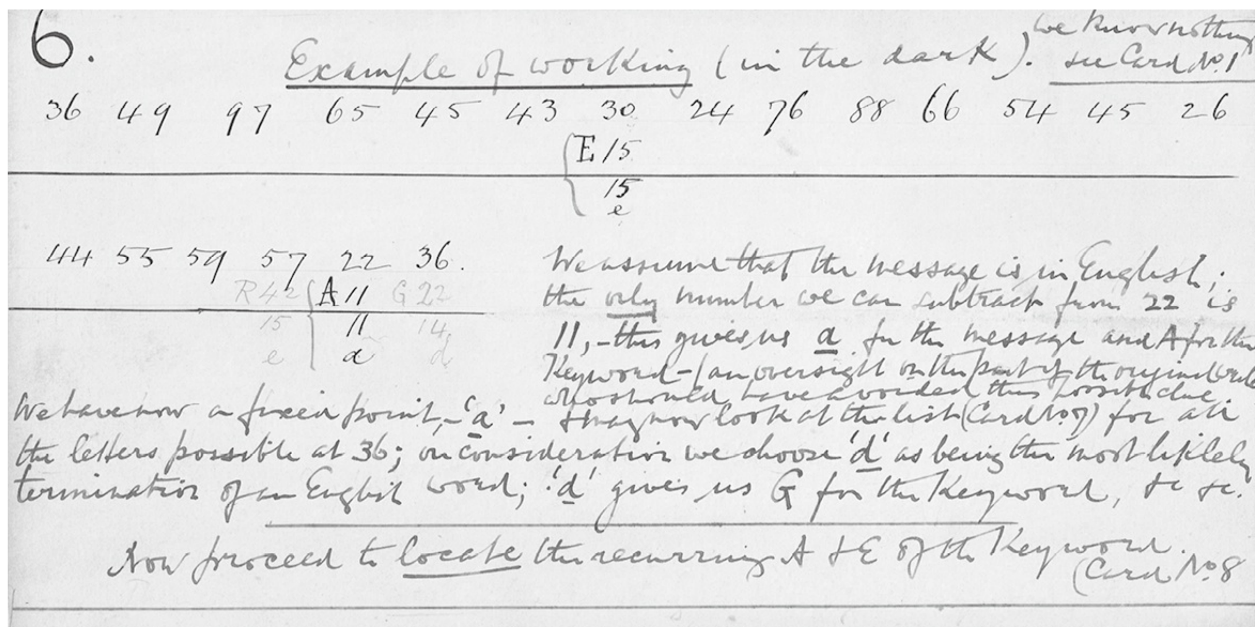


图3-17 第6张卡片：埃尔加开始破译这条信息

密码中剩下的数字都有不止一种可能性。在第7张卡片上，埃尔加用穷举法列出了每个数字的所有可能性。比如，密文中的第二个数字是49，49可以通过以下几种方式产生：14 + 35，15 + 34，或者24 + 25。当然，上述这三种可能性中的两个数字还可以调换顺序，这样又得到另外三种可能性，比如14 + 35也可以是35 + 14。但是，埃尔加并不在意上述几对数字对应的字母究竟哪个来自明文信息，哪个来自关键词，他只想知道密码中究竟出现了哪几对字母。埃尔加把相加能得到49的几对数值按数字顺序写了出来，并且转换成了对应的字母：D、E、I、K、O和P。密文某些位置上的数值可能对应于几种不同的字母对，但是没关系，因为埃尔加还有另外一个撒手锏没有使用。

在第8张卡片上，埃尔加列出了关键词中所有可能为字母A或者字母E的位置。之所以选择这两个字母，是因为埃尔加已经找到了这两个字母必须出现的位置（见第6张卡片）；并且，通过斯库林给出的例子，可以判断密码的关键词会多次重复。如果能够通过以上这些信息确定关键词的长度，那么就离找到关键词越来越近了。密码破译者经常都只能这样小步地向目标前进。要做一名密码分析师，就必须有耐心和恒心，坚持不懈地挖掘密码中的小漏洞，直到最终获得完整的解答。

7. Table of possible letters. (under each number)

1. 36
11 a, 12 b, 13 c, 14 d, 15 e, 21 f, 22 g, 23 h, 24 i, 25 k

2. 49
14 d, 15 e, 24 i, 25 k, 34 o, 35 p

3. 97
42 r, 43 s, 44 t, 45 u, 52 w, 53 x, 54 y, 55 z

4. 65
11 a, 12 b, 13 c, 14 d, 21 f, 22 g, 23 h, 24 i, 31 l, 32 m, 33 n, 34 o
41 q, 42 r, 43 s, 44 t, 51 v, 52 w, 53 x, 54 y

5. 45
11 a, 12 b, 13 c, 14 d, 21 f, 22 g, 23 h, 24 i, 31 l, 32 m, 33 n, 34 o

6. 43
11 a, 12 b, 21 f, 22 g, 31 l, 32 m

7. 30
15 e

E

8. 24
11 a, 12 b, 13 c

9. 76
21 f, 22 g, 23 h, 24 i, 25 k, 31 l, 32 m, 33 n, 34 o, 35 p
41 q, 42 r, 43 s, 44 t, 45 u, 51 v, 52 w, 53 x, 54 y, 55 z

10. 88
33 n, 34 o, 35 p, 43 s, 44 t, 45 u, 53 x, 54 y, 55 z

11. 66
all letters are possible

12. 54
11 a, 12 b, 13 c, 21 f, 22 g, 23 h
31 l, 32 m, 33 n, 41 q, 42 r, 43 s

13. 45
11 a, 12 b, 13 c, 14 d, 21 f, 22 g, 23 h, 24 i
31 l, 32 m, 33 n, 34 o

14. 26
11 a, 12 b, 13 c, 14 d, 15 e

15. 44
11 a, 12 b, 13 c, 21 f, 22 g, 23 h
31 l, 32 m, 33 n

16. 55
11 a, 12 b, 13 c, 14 d, 21 f, 22 g, 23 h, 24 i
31 l, 32 m, 33 n, 34 o, 41 q, 42 r, 43 s, 44 t

17. 59
14 d, 15 e, 24 i, 25 k, 34 o, 35 p, 44 t, 45 u

18. 57
12 b, 13 c, 14 d, 15 e, 22 g, 23 h, 24 i, 25 k
32 m, 33 n, 34 o, 35 p, 42 r, 43 s, 44 t, 45 u

19. 22
11

A

20. 36
11 a, 12 b, 13 c, 14 d, 15 e, 21 f, 22 g, 23 h, 24 i, 25 k.

图3-18 第7张卡片：埃尔加用穷举法列出了剩下的可能性

埃尔加并没有在第8张卡片的空白处详细记录他究竟如何确定出关键词的长度。也许他是尝试了多种可能性，直到找到一种和已知情况能完全吻合的情况。一开始，埃尔加可能最先测试长度为2的关键词：由于已经知道关键词第19位上的字母是A，因此如果关键词的长度为2，就意味着关键词的所有奇数位上都必须是字母A。但是关键词的第3位不可能是字母A，因此可以推测出关键词的长度不能是2。接着，埃尔加再以同样的方式测试关键词长度是否可能为3。如果关键词的长度为3，那么关键词第7位上的字母E意味着关键词第1、4、7、10等位上都必须是字母E。然而，关键词的第4位上的字母不可能是E，因此关键词长度为3的可能性也可以被排除了。接下来，需要继续测试关键词长度是否可以为4。关键词第7位上的字母E意味着关键词第3位（以及其他一些位置）上的字母也是E，但是第3位上的字母不可能是E，因此排除关键词长度为4的可能性。接下来研究关键词长度是否可以为5。如果关键词长度为5的话，关键词第7位上的字母E意味着关键词第2、7、12、17位上也必须是字母E，然而第12位上不可能是字母E，因此排除关键词长度为5的可能性。再接下来，如果关键词长度为6，第7位上的字母E意味着第1、13、19位必须是字母E，但是第13位不可能是字母E，并且已知第19位上是字母A，所以关键词长度也不可能是6。还记得我说过密码分析师必须有耐心和恒心吗？接下来，我们测试关键词长度为7的可能性。我们终于确定这个长度是可行的。如果关键词长度为7，并且我们已知第7位上的字母为E，那么第14位上也必须是E，这是可行的。同时第19位上的字母为A，这说明第12位和第5位上也必须是A，这也是可行的。在第8张卡片上，埃尔加把新发现的这几个字母写在了第14位、第5位和第12位上，并且画圈表示强调。

现在，关键词的长度看上去似乎是7，于是埃尔加在卡片上写出了他已知的关键词形式。用x来表示关键词中的未知字母，那么关键词的形式可以记作xxxxAxE。

现在，我们再回头去看第7张卡片。在第7张卡片上，埃尔加列出了明文第18位和第20位上的若干可能性（他已经知道第19位上的字母是A）。如果我们画一个表格，用其中的3列分别表示第18、19、20位上字母的各种可能性，就可以得到以下结果：

第18位	第19位	第20位
B	A	A
C		B
D		C
E		D
G		E
H		F
I		G
K		H
M		I
N		K
O		
P		
R		
S		
T		
U		

第18位上的字母共有16种可能性，第19位上的字母只有1种可能性，第20位上的字母共有10种可能性，因此这三个位置上的内容有

16×1×10共160种可能性。但是，这三个位置是信息结束的最后三个字母，因此在这160种组合中，有许多种组合事实上是不太可能出现的。比如，你认为一条信息可能以UAI结尾吗？在第8张卡片上，埃尔加写道：“假设信息结尾处的三个字母是E、A、D……”这是一种不错的猜测！然而，也许埃尔加在写下这句话之前已经尝试过其他各种可能性了，E、A、D是他排除其他可能性后得到的结果。第18、19、20位上的三个字母的可能组合只有160种，因此一个人只要有足够的耐心，就可以把它们全部尝试一遍。不管怎么样，明文信息的第20位上的字母是D（根据之前给出的字母数字转换表格，D ＝ 14），这就意味着关键词在该位置上必须是22（G），否则密文第20位上就不是36了。根据这一点，埃尔加判断：关键词的形式是xxxxAGE。事实上，如果埃尔加用同样的方法分析明文信息第18位上的字母E，那么他还可以进一步猜出关键词的形式为xxxRAGE。埃尔加十分喜欢玩填字游戏，在这个过程中培养出的技能或许帮助他判断出了密码关键词的剩余部分。埃尔加在卡片上写道：经过“进一步的试验”，他判断出密码的关键词是“COURAGE（勇气）”。

图3-19 第8张卡片：埃尔加判断出关键词

N.B. – Having ascertained beyond doubt that 30 represent E and 22 = A: the next proceeding is to discover in what order these letters recur: it is useless to count forward from A or E as the end of the key word does not necessarily coincide with the end of the Text.

图3-20 第8b张卡片：关于判断关键词长度的更多细节

在第8张卡片背面，埃尔加给出了关于关键词长度判断的更多细节。然而，埃尔加的笔迹实在是太难认了，与其试图破译他的笔迹，还不如自己想办法判断关键词的长度。

在确定了关键词以后，埃尔加利用转换表格把关键词从字母转化成数字，再把关键词对应的数字从密文中减去。这样就得到了这段密码的最终破译结果。埃尔加把最终的破译结果写在了第9张卡片上。

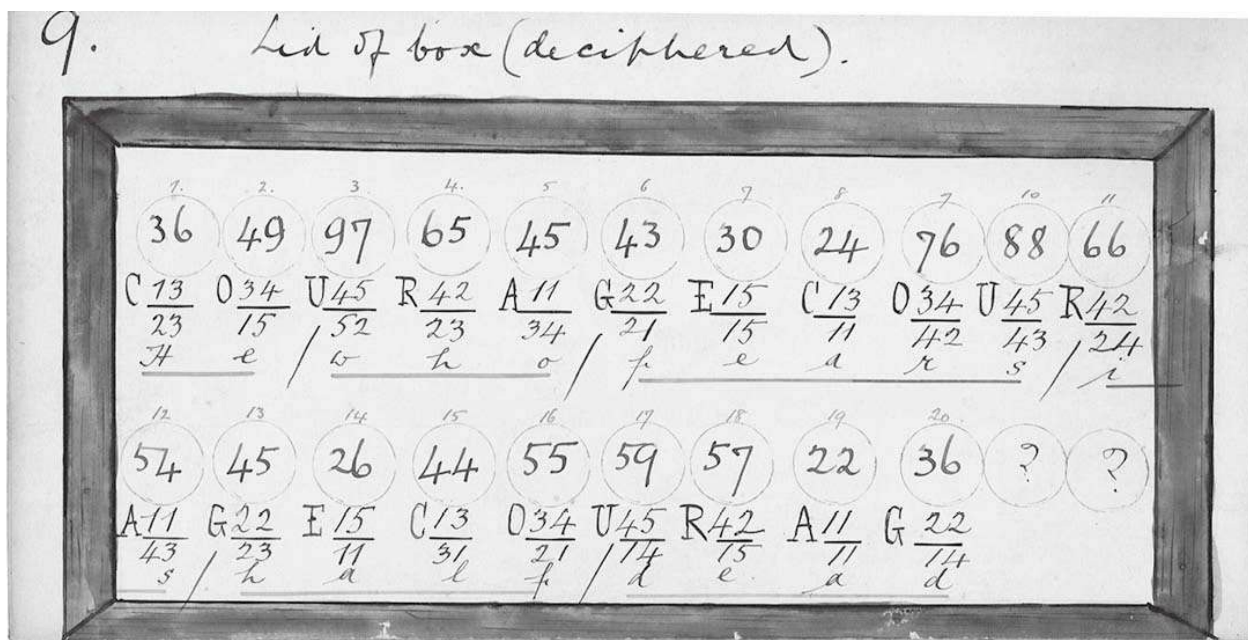


图3-21 第9张卡片：埃尔加给出了密码的解答

第9张卡片上的内容有些太拥挤了，因此我把计算的过程（更清楚地）誊写如下：

```
   36 49 97 65 45 43 30 24 76 88 66 54 45 26 44 55 59 57 22 36
 -  C  O  U  R  A  G  E  C  O  U  R  A  G  E  C  O  U  R  A  G
   13 34 45 42 11 22 15 13 34 45 42 11 22 15 13 34 45 42 11 22
   ___________________________________________________________
 = 23 15 52 23 34 21 15 11 42 43 24 43 23 11 31 21 14 15 11 14
    H  e  w  h  o  f  e  a  r  s  i  s  h  a  l  f  d  e  a  d
```

至此，我们终于知道，这段密码的明文信息为："He who fears is half dead.（一个人一旦感到恐惧，他就已经死去了一半。）"

据尼克·佩林称："解开这段密码给埃尔加带来了极大的愉悦，以至于事后他把这句话刷在了地板上。"[注]近10年以后，破译这段密码的经历仍然是埃尔加最得意的一段回忆，他把这段故事告诉了他的第一位传记作者。这本传记出版于1905年，书中写道："在坐火车旅游的时候，

他把密码当作一种娱乐。约翰·霍尔特·斯库林设计了一个密码来挑战全世界，而埃尔加成功破译了这个密码。”[注]

虽然这个密码的破译结果非常有趣，虽然我事先说过本书中也会出现一些已经被破解的密码，但是本书的重点还是“未解之谜”。除了以上这些卡片之外，还有另外一张卡片能把斯库林密码的解法和埃尔加设计的未解之谜（多拉贝拉密码）联系起来，请见图3–22。

请注意，这张卡片上有一行弯弯曲曲的符号，总数是10个。此外，这张卡片上还写有“Cryptogram（密码）”的字样，“Cryptogram”一词恰好也有10个字母。一开始，我以为这张卡片上的“Cryptogram”是明文，而那些弯弯曲曲的符号是密文。然而我很快就认识到，在“Cryptogram”一词中，字母R出现了两次，而10个弯弯曲曲的符号却各不相同，没有任何一个符号出现过两次。

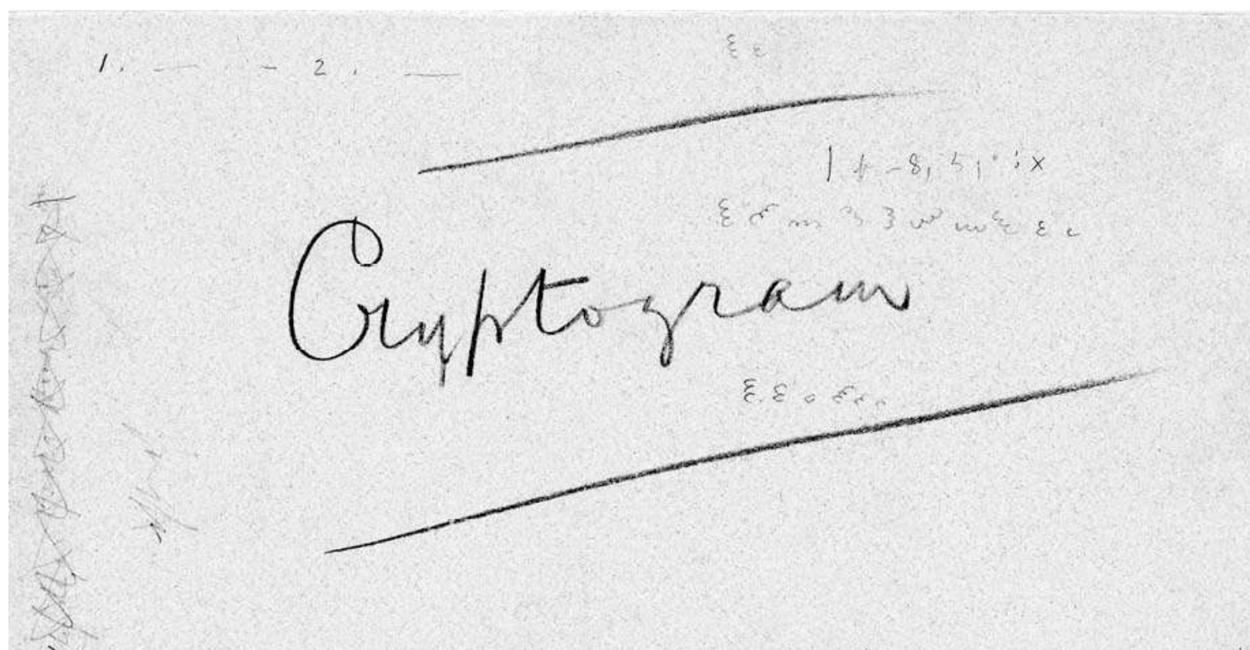


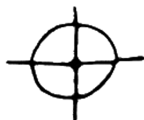
图3-22 写有“cryptogram（密码）”字样的卡片

当我仔细观察这张卡片上的弯曲的符号时，我发现这几个符号的排列有一定规律，就好像第一个符号慢慢向一边倒去，然后摔倒，接着又翻了一个面——好像在做前滚翻一样。最后，当这个符号几乎要回到初

始状态的时候，符号的长度减少了。

我们当然可以把这些内容看成是漫不经心的涂鸦，但是我们知道，不管是在埃尔加破译斯库林密码之前还是之后，这些弯弯曲曲的符号对埃尔加而言都是有意义的。因此，似乎有理由假设这张纸上的这些弯弯曲曲的符号也是有意义的。由于这行弯弯曲曲的符号出现了上述这种依次向前翻倒的规律，所以这行符号似乎并不代表一个加密单词。然而，结合背景信息来考虑，这张纸上的10个弯弯曲曲的符号可能具有相当的重要性。埃尔加会不会是想用这些符号来代表从0到9的10个数字呢？如果埃尔加想到了以上这个主意，他就可以用这些符号来书写一段“无政府主义密码”。克里斯蒂安·施里德（Christian Schridde）曾经提出这种怀疑。但是，我认为这种想法恐怕并不能帮助我们破译多拉贝拉密码，因为在多拉贝拉密码中出现的弯弯曲曲的符号并不止上述10种。但是，也有一种可能性是，某些数字可以与多种不同的弯曲符号相对应。也就是说，如果埃尔加是加密者，那么在写下某个特定的数字时，他希望能从若干种可能性中自由选择一种。当然，图3–22中的卡片并不能证明埃尔加确实有这种想法。另一种反对把斯库林密码和多拉贝拉密码联系起来的理论是：既然埃尔加已经成功破译了斯库林密码，这就说明埃尔加已经知道斯库林的加密方式是不安全的，既然如此，当埃尔加自己对文字加密时，他又怎么会去采用一种不安全的加密系统呢？

埃尔加的家庭游戏



1917年8月20日，在一封埃尔加写给女儿卡里斯（Carice）的信中，他又使用了一种与上述密码都不相同的密码。我把这段密码及密码的上

下文摘录如下注：

I was glad to get your letter because I feared the North End road has para pary parri p (I will) pare paryli parali paralyside pare paralysed your writing thumb — I had not heard for deax — I am reading GK phuriosli — hence

[很高兴收到你的来信，因为我担心北端路会para pary parri p（我将会）pare paryli parali paralyside pare令你写字的拇指麻痹。我没有听到deax的消息——我正在阅读GK phuriosli——于是]

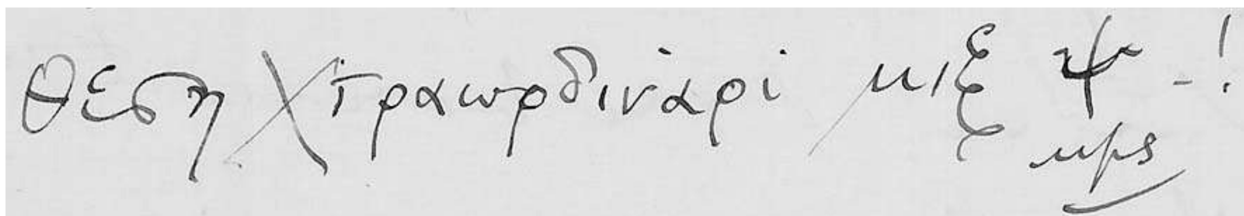


图3-23 一封包含埃尔加的另一段密码的书信

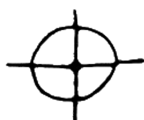
在本书的第2章中，我们曾经提到恺撒使用过的密码。图3–23中出现的密码与恺撒使用的密码十分类似。一位不认识希腊文的读者可能会拿出一本希腊语词典，并试图查出图中文字的意思，但是这样做是不会有结果的。而一位更聪明的读者可能会用这些希腊字母所对应的拉丁字母来替代它们，这样就可以得到一句有意义的话："these extraordinary mix-ups!（这些非凡的混合体！）"

埃尔加非常喜欢玩这类文字游戏。事实上，他女儿的名字也是某种文字游戏的产物。在埃尔加的女儿出生之前，埃尔加把妻子的名字卡罗琳·艾丽斯（Caroline Alice）缩写成了卡里斯（Carice），放在一首歌的献词里。此外，埃尔加还给他的一栋房子起名为"Craeg Lea"，这里也玩了一个文字游戏。"Craeg Lea"来自对以下一些字母的重新排列，包括：埃尔加姓名的首字母缩写，埃尔加妻子姓名的首字母缩写，以及埃尔加

姓的剩余部分——“Alice Carice Edward Elgar”中画了下划线的几个字母。

然而，在以上所有这些文字游戏中，埃尔加并没有把字母转化成弯曲的符号。

一个残忍的恶作剧？



在这些破译多拉贝拉密码的努力都失败以后，我们很容易得出这样的结论：也许多拉贝拉密码只是一个恶作剧，也许埃尔加只是随机地把一堆符号放在一起，背后并没有隐藏什么意思。埃尔加写给多拉的这封信既不准备卖出大价钱（像我们第1章中提到的伏尼契手稿一样），也不打算指出什么宝藏的埋藏地点［参见《未解之谜（下）》第9章中的比尔密码］。在这种情况下，如果这段密码确实是一个恶作剧，那么这个恶作剧的动机也是残忍的，也就是说埃尔加写这段密码是为了戏弄多拉并且浪费她的时间。因此，一个问题产生了：埃尔加是一个残忍的人吗？关于这个问题，与其研究外人的证言，我们不妨先看一看埃尔加本人写的一封信。[注]

巴滕霍尔庄园，伍斯特郡

1928年3月27日

Dgck[注][注]

首先，星期日下午我们去了S-on-A（一切都非常好）。在回来的路上我们“杀死”了一条狗。这条狗跑到了外面，我也跑到了外

面。然后一个非常友善的人说这条狗属于一个跛脚的男孩子，这条狗是他的宠物，他会和这条狗一起睡觉。早就有人告诉这个男孩，不要让他的狗跑到外面——完全不是我们的错——他们把这只可怜的小动物带到他们的花园中，跛脚的男孩子一边无助地哭着一边逃跑了。整件事都太悲惨了——然后就是快乐！今天早晨（星期二）我收到了这份附件。

你将会收到这个谜题。你已经比我多做对一个，比如29→29↓。我推断出：water-ice=SORBET（水一冰=果汁冰水）——减去ore你就会得到SBT——但这看起来也不对。

~~我回复了沃克·巴纳德的信，如果你还没回，你可以写。~~

不，我没有——我会给他们送一张便条，告诉他们你替我询问了，看到了吗？

这里大家都好，玛丽也好些了：今天她能走着去买东西了，这可能是一件好事。

我拜访了弗兰克三次。他毫无希望。

爱你，
E. E.

好吧，埃尔加可真爱玩填字游戏啊！为了让读者放下对小狗命运的担心，我可以告诉大家这条狗最后完全康复了。这个故事的奇怪之处在于，虽然埃尔加看起来对别人家的狗漠不关心，但他对自己的狗却是非常喜爱的。下面我再给读者讲另一则关于埃尔加的故事，从这个故事里我们可以看出埃尔加有时是如何与家人互动的。

星期日的整个上午，E. E.和耶格先生都把自己关在书房里。我从教堂回来，顺路把卡里斯从学校接了回来。当我们回到家时，发现他们还在忙。“木柱”[注]来我们家吃午餐，一切都很有趣。当他们走进餐厅的时候，E. E.看见卡里斯正站在她的椅子边上等着。

“你好，鱼脸蛋！你好吗？”

“我很好，谢谢你，爸爸。”

“我很好，谢谢你，爸爸。”E. E. 用一种尖锐的声调模仿道。而卡里斯这个可怜的孩子在听完这种嘲讽以后还要做饭前祷告。注

所以，埃尔加有时确实是个残忍的人。那么他对多拉残忍吗？不幸的是，答案是肯定的。不管是在身体上还是在感情上，埃尔加都曾经残忍地对待过多拉。多拉写过一本关于她和埃尔加的关系的书，她在书中提供了这样一个例子：

我们一起吃了晚餐。他全程一句话都不说。他要么盯着自己的盘子，要么就用一种非常紧绷的表情盯着他面前的空气。他的脸十分苍白扭曲，看起来很疲惫。当甜点吃到一半的时候，他突然把椅子向桌子推去，当时我的手正好放在桌子上，他的椅子重重地撞到了我的手。而他转身离开了餐厅。他撞上书房的门，还用钥匙把门从里面反锁起来。一瞬间我产生了这样的念头：“他锁门是为了不让我进去。”我诧异地看着女主人。

女主人回答说：“自从书房搬到楼下，他总是把自己锁在书房里。这样他觉得安全一些！”

事实上，我虽然在他们家做过几次客，但我从没进过他的书房，除非书房的门开着，或者有人叫我或派我进去。

“哦，亲爱的多拉，看看你可怜的手！埃尔加真是太坏了，真的！”

“我的手伤得没有看起来那么严重，”我一边说一边揉着自己的手，“我想它很快就会好了。”注

从多拉叙述的这个故事里，我们没有办法知道埃尔加是不是故意弄

伤了多拉的手。但显然埃尔加夫人相信，埃尔加是故意这么做的。然而，埃尔加后来自己为我们解开了这个疑团。在突然离席之后，埃尔加又重新回到了餐厅里，并且，这时的他变得稍微健谈了一些。

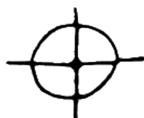
> “一开始我希望你不会。但是，在吃晚饭的过程中，我又希望你会。最后我走开了。你赢了。所以我才那么重地用椅子撞你的手。你的手疼吗？我是故意叫你疼的。”他拿起我的手检查起来。[注]

多拉又一次假装自己伤得没那么重。几年以后，埃尔加所写的《谜语变奏曲》中出现了描写多拉的变奏，这段音乐一定给多拉带来了一些情感上的伤害。但是多拉又一次选择了同样的处理方式：假装自己伤得没那么重。

> 在前文中，我已经谈过我第一次听到用钢琴演奏的这首曲子和由交响乐团演奏时的感想了。我完全不知道那是什么意思。直到很多年以后，我才意识到我就和R. B. T. 一样，是E. E. 的那种顽皮的幽默感的受害者。[注]在我小的时候，我有时说话口吃得厉害。我和很多人一样为此深感烦恼，这对我来说是一种极大的折磨。我很高兴，现在这件事情已经在某种程度上成为过去。埃尔加的幽默是建立在我的痛苦之上的，他写得如此巧妙，任何人都会跟他一起嘲笑我——如果他们理解乐曲中的意思的话。但不管怎么样，以前从来没有人写出过像这段间奏曲一样的作品，在埃尔加以后，也不会有人写出这样的作品，知道这一点还是很让我满足的。[注]

关于多拉和埃尔加的关系，埃尔加的传记作者伊恩·帕罗特（Ian Parrott）写道：“她（多拉）总是过度强调埃尔加快乐的一面。”[注]

用莫尔斯电码破译



我们知道，多拉对莫尔斯电码有一定的兴趣，她甚至还将莫尔斯电码写在她1899年日记中的空白页。此外，埃尔加也喜欢玩莫尔斯电码。在2004年发表于《新科学家》（*New Scientist*）杂志上的一篇文章中，凯文·琼斯（Kevin Jones）这样写道：

> 1901年埃尔加给多拉的这封信中可能也用到了莫尔斯电码。在这段信息中，埃尔加加入了一些来自他的《谜语变奏曲》的简短而独特的音乐动机[注]。具体来说，这封信中引用了多拉贝拉变奏中的一个片段，还引用了乐曲开篇主题的起始段落。信中的这段内容依次是："Whether you are as nice as（你是否如……一样美好）"，三个短音符，又三个短音符，"or only as unideal as（或者只如……一样不理想）"，两个短音符，两个长音符。如果用莫尔斯电码进行破译，那么这些神秘的音符就变成了SS和IM，于是这段话就成为："Whether you are as nice as sugar and spice or only as unideal as I am（你是否如糖和香料一样美好，或者只和我一样不理想）。"[注]

我将这封信中提到的几个动机展示在图3–24中。[注]

Whether you are as nice as



or only as unideal as



Eh? No. Perhaps??

图3-24 音乐莫尔斯电码

虽然多拉贝拉密码中那些弯弯曲曲的符号看起来并不像莫尔斯电码，但是上图中的这些音乐动机看起来也同样不像莫尔斯码！我们可以通过许多不同的方法把多拉贝拉密码中的符号分成两组，其中一组代表点，另一组代表横线。但是对于任意一种分组方法，都可以进行多种不同的解读——因为莫尔斯电码还需要另一种符号。如果没有把字母分开的分隔符号，我们就无法知道前一个字母在何处终止，后一个字母在何处开始。除了字母与字母间的分隔号以外，发莫尔斯电码的时候还必须用到另外一种符号——一个长长的停顿，来把单词与单词分开。

此外，任何想要以某种方式用莫尔斯电码来破解多拉贝拉密码的人还应该注意另外一个问题，那就是莫尔斯电码有三种不同的版本：美国版本，欧洲大陆版本，以及国际版本。

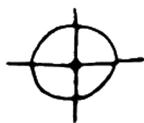
埃尔加从来没有向多拉表示过信中这些弯弯曲曲的符号代表莫尔斯电码，但是一般来说，埃尔加似乎并不希望看到他自己创造的谜题或者密码被别人破解。在本书前面的内容中，我们曾经提到埃尔加给自己的一处房子起名“Graeg Lea”，当时我讲这个故事是为了证明埃尔加十分喜欢玩文字游戏。现在我们又要讲另外一段关于这个故事的逸事，从这段逸事中我们可以看出，埃尔加不希望任何人解开自己的谜题。

爱德华给这座房子起名为“Graeg Lea”，并且问我能不能猜出

他想到这个名字的方法。由于某种特殊的好运气，我意识到破解这个问题的关键在于“Graeg”这个词不平常的拼法，并发现这个名字是由“(A)lice (C)arice (E)dward ELGAR”这几个字经过字母顺序重排而得到的。我想由于他的谜题被我解开了，爱德华有些不高兴。㊟

后来，多拉和一个叫理查德·鲍威尔（Richard Powell）的人结了婚。理查德·鲍威尔认为埃尔加的《谜语变奏曲》中的隐藏主题是《友谊地久天长》（*Auld Lang Syne*），并且提出了相当具有说服力的解释。多拉最后一次和埃尔加交谈时，埃尔加告诉她，她丈夫的上述理论是错误的。然而，后来多拉向别人透露，埃尔加并不善于说谎，从埃尔加的行为中多拉可以看出，事实上理查德的猜测是正确的。对于多拉来说，说出这件事情涉及很强的个人感情，因为她很难接受埃尔加向她说谎这一事实。在对别人披露这件事情时，多拉要求对方保守住这个秘密。对方也履行了他的诺言，直到多拉去世后许多年，他才说出实情。

最后的失败



如果埃尔加的密码只是一种去掉了单词间空格的MASC密码，那么计算机自动程序应该能够很快地破解它。但是，事实上计算机程序却完全没有办法破解这段密码！我认为，看看下面这封埃尔加的女儿卡里斯写给埃尔加的信也许能帮助我们找到其中的原因。㊟

The Mount

Malvern

Jeudi [2 Oct. 1902]

My dearest Mother & Faser

I hope zu are bof enjoying yoursouses vesy much.

I’se dood & happy & cean & well, & busy & polite.

Dreffful many sanks for the beauful card.

I had to put Jeudi on my letter, because I have been talking French & cannot get it out of my head.

I hope “Gerontius” will be beautiful to-day.

Our class & the other are going to Mr. Montagnon for Grammar this evening. I am looking forward to it.

I am going to have a lovely music-lesson “KEKKY”, & I shall show Miss Reynolds “the” postcard.

Dreffful much love from your loving little ~~fille~~ daughter

Carice

这封奇怪的信大体翻译如下：

写于山区

马尔文

星期四（1902年10月2日）

我亲爱的爸爸、妈妈，

我希望你们两人过得都很愉快。

我很好，很高兴，很干净，很健康，很忙碌，很有礼貌。

非常感谢你们给我的漂亮的卡片。

我必须在这封信里写上“Jeudi”这样的词，因为我一直说法语，我满脑子都是法语。

我希望“杰隆修斯”今天会很美丽。

今天晚上我们班和其他班的同学都会去蒙塔尼翁先生处上语法课，我很期待。

我将要上一堂美好的音乐课“KEKKY”，我会给雷诺兹小姐看“那张”卡片的。

许多许多的爱，来自爱你们的小女儿。

卡里斯

这封信里不仅有许多拼写错误，而且还有一个自创的单词（KEKKY）。有些词虽然在这封信里被拼写对了，但是在其他信里却被故意拼错。埃尔加经常用这种奇怪的方式和家人进行书信交流！

此外，埃尔加还经常把两个相邻单词的首字母或者首音节进行交换。通过这种方法，他创造出了Histish englory，Uther or Fancle，exwrite the skusing，busted a sculp，Bung yirds，Kig-spin，clise wub，I’m waiting for my dimple sinner & am hungfully paingry，It’s raining dots & cags，oracular jerkations，Philharmonic Qreisler in the Kueen’s Hall，I smowed & biled，chiserable meque，a box of pam，jickles fished meat & mated pot!，preieping wedderations，hates and dours，dimes and tays，以及tace and plimes[注]。[注]

我个人怀疑，计算机自动程序之所以无法破译多拉贝拉密码，是因为多拉贝拉密码中含有许多拼写错误的单词，还含有埃尔加和他的家人自己创造出来的单词。如果我的这种猜测正确的话，我们可以把埃尔加现存书信中的这些怪词收集整理出来，统一加入标准词典文件中，这样就能产生一个新的词汇数据库。有了这个数据库，计算机自动程序就有

可能成功破译多拉贝拉密码。



图3-25 为了纪念埃尔加，他的头像出现在20英镑面值的纸币上

1999年6月，英格兰发行了如图3–25所示的纸币。在1999年6月到2010年6月30日之间，上图中的纸币都是英国市场上合法流通的货币之一。埃尔加并不是因为他在密码方面的造诣而获得此项殊荣的，但是，在我们这本关于未解之谜的书中，肖像出现在货币上的人物并不止埃尔加一位。在《未解之谜（下）》的第8章中，我们还将提到另一位出现在货币上的人。那么，在阅读第8章之前，读者能猜出那个人是谁吗？

---

1. This is actually a series of six marches titled Pomp and Circumstance Military Marches, of which the Trio section, “Land of Hope and Glory,” of the first is played at many American graduations.
2. Edward Elgar, My Friends Pictured Within (London: Novello and Company Ltd, 1946).
3. John C.Tibbetts, “John C.Tibbetts Interviews Eric Sams,” available online at http://www.ericsams.org/index.php/interview-by-john-c-tibbetts.
4. Ron Rosenbaum, “A Visit with an Avenging Angel,” The Shakespeare Wars (New York: Random House, 2008), 66–75, available online at http://www.ericsams.org/index.php/ron-rosenbaum -the-avenging-angel.

5. John C.Tibbetts, “John C.Tibbetts Interviews Eric Sams,” available online at http://www .ericsams.org/index.php/interview-by-john-c-tibbetts.

6. Solution #04, revised as #36, posted at http://unsolvedproblems.org/index_files/Solutions .htm.

7. E-mail received by author on June 19, 2015.

8. Found in an odd book by one of the people who claimed a solution to the Voynich manuscript: Joseph Martin Feely, Electrograms from Elysium: A Study on the Probabilities in Postmortuary Communication through the Electronics of Telepathy and Extrasensory Perception, Including the Code of Anagrams in the Purported Sender’s Name (New York, 1954), 246.

9. See https://www.cqu.edu.au/about-us/staff-directory/profiles/higher-education-division/higher -education-division-honadjunct-appoint/robertst and http://unsolvedproblems.org/S12x.pdf.

10. Jerrold Northrup Moore, Edward Elgar: A Creative Life (Oxford, U.K.: Oxford University Press, 1984), 114. The passage also appears online at http://www.benzedrine.ch/dorabella.html.

11. John Holt Schooling, “Secrets in Cipher IV. From the Time of George II. to the Present Day,” The Pall Mall Magazine 8, no. 36 (April 1896): 608–18, p. 618 cited here.

12. http://www.ciphermysteries.com/2013/10/09/elgars-little-cipher.

13. Robert J.Buckley, Sir Edward Elgar (London: Ballantyne, Hanson & Co., 1905).

14. The Elgar Birthplace Museum, L189.

15. The Elgar Birthplace Museum, L296.

16. “Dgck”是“亲爱的查克”的缩写，查克指埃尔加的女儿卡里斯。——译者注

17. This was short for “Darling Chuck,” where Chuck was Elgar’s daughter Carice.

18. 指埃尔加的一位朋友特罗伊特·格里菲思（Troyte Griffith）。因为他又高又瘦，所以埃尔加用九柱戏（一种英国室内游戏）的木柱来称呼他。——编者注

19. Mrs. Richard Powell, Edward Elgar: Memories of a Variation, 4th ed., rev. and ed. Claud Powell, addendum Jerrold Northrop Moore (Aldershot, Hants, U.K.: Scolar Press, 1994), 36.

20. Powell, Edward Elgar, 4th ed., 90–91.

21. Powell, Edward Elgar, 4th ed., 93.

22. R.B.T. was Richard Baxter Townshend. Elgar’s variation for Townshend ridiculed Townshend’s inability to control his voice in the amateur theatre productions he performed in.

23. Powell, Edward Elgar, 4th ed., 132–33.

24. Ian Parrott, Elgar (London: J.M.Dent and Sons Ltd., and New York: Farrar, Straus and

Giroux, Inc., 1971), 122.

25. 音乐动机（motif）是指音乐作品中具有特征性、经常反复出现的短小的音乐片段。——译者注

26. Kevin Jones, “The Puzzling Mr. Elgar,” New Scientist 184, no. 2479 (December 25, 2004): 56.

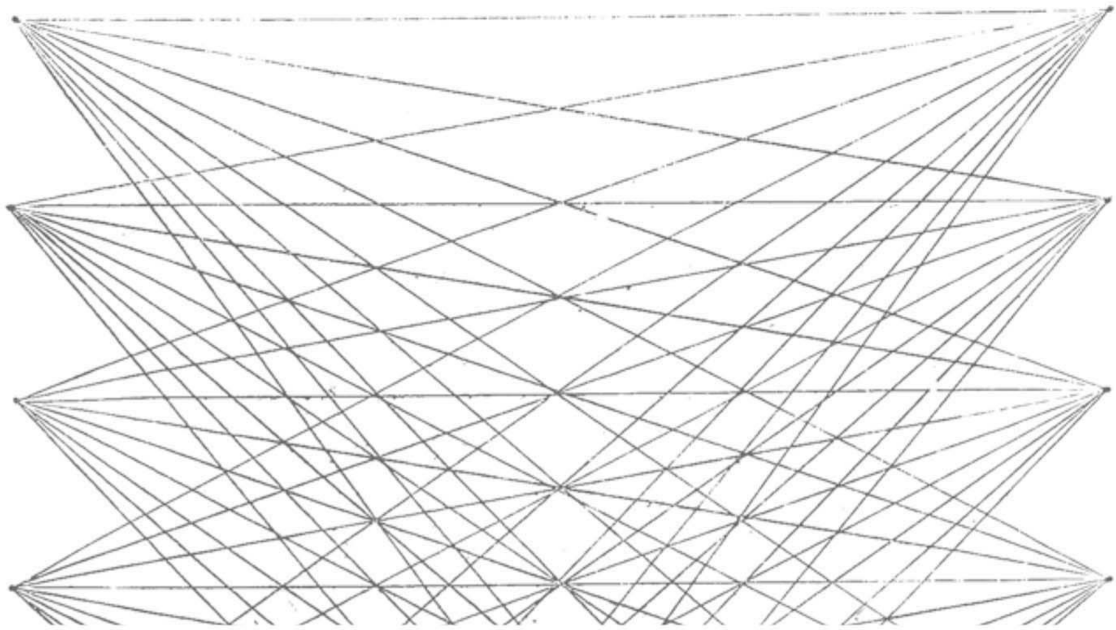
27. Mrs. Richard Powell, Edward Elgar: Memories of a Variation (London: Oxford University Press, 1937), 35.

28. Rosa Burley and Frank Carruthers, Edward Elgar: The Record of a Friendship (London: Barrie and Jenkins, 1972), 132.

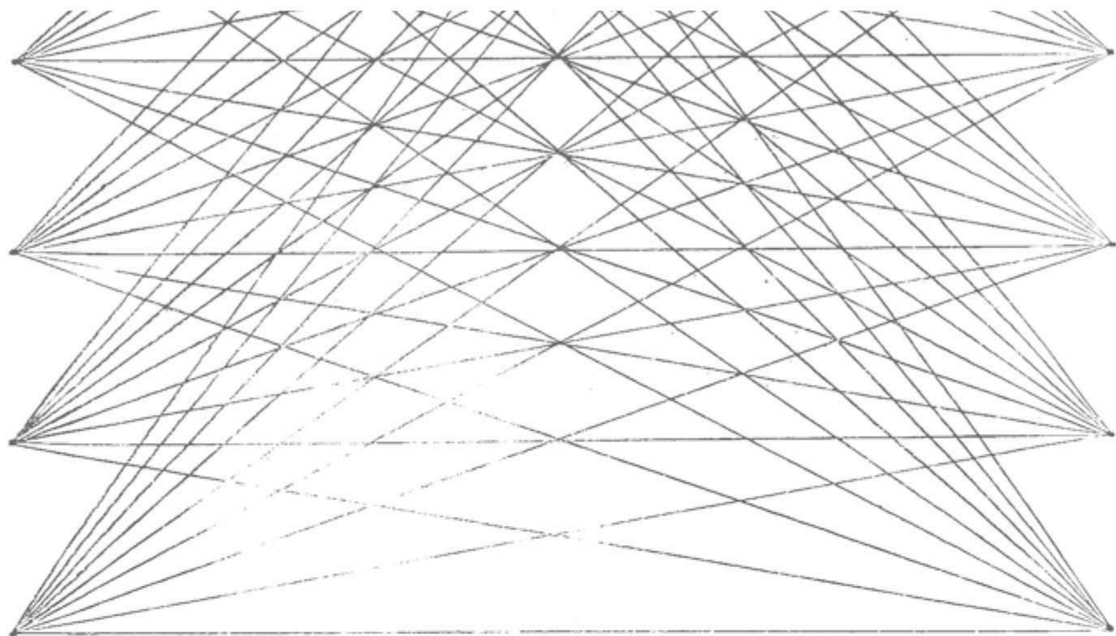
29. Elgar Birthplace Museum, L1104.

30. 上面各个词组或句子在交换字母之前的意思分别为：英国历史，父亲或叔叔，写信请求原谅，打碎了一个雕塑，小鸟，猪皮，聪明人俱乐部，我在等待简单的晚餐但我已经快饿死了，外面倾盆大雨，幽默的演说，皇后厅的克莱斯勒交响乐团，我微笑着鞠了躬，痛苦的代价，盒子里装满了果酱、腌鱼、成对的罐子，准备婚礼，日期和时间，时代，地点和时间等。——编者注

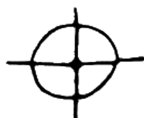
31. Martin Bird, ed., Darling Chuck, The Carice Letters, Edward Elgar: Collected Correspondence, ser. II, vol. 1, Elgar Works (Chippenham, Wiltshire, U.K.: Antony Rowe Ltd., 2014). Examples from pp. 145, 159, 160, 162, 163, 164, 164, 164, 168, 182, 192, 201, 204, 237, 272, 381, 381, and 381, respectively.



第4章 黄道十二宫杀手密码



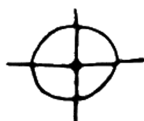
第一次约会



根据目前已知的情况，黄道十二宫杀手的故事似乎开始于1968年12月20日星期五。在这个不幸的夜晚，年仅16岁的少女贝蒂·卢·詹森（Betty Lou Jensen）离家赶赴她人生的第一次约会。贝蒂的约会对象是17岁的戴维·阿瑟·法拉第（David Arthur Faraday）。戴维不仅是一名成绩优秀的好学生，还是学校摔跤队的成员。两人将车停在加利福尼亚州瓦列霍市的赫尔曼湖路附近，此处是当地著名的情人巷。

贝蒂和戴维于当晚11：10至11：15之间遭受了袭击。凶手用枪顶住戴维的头，并扣动扳机，杀死了车中的戴维。贝蒂逃出了汽车，但在她试图逃走的过程中，凶手对着她的背部连开5枪，将她射杀。两名年轻人都不幸死亡。事后，警察在案发现场发现了10枚0.22英寸口径的弹壳。

第二起攻击案



1969年7月4日刚刚结束，7月5日只过去了几分钟，杀手又发起了第二次袭击。此次袭击的地点是瓦列霍市的另一处情人巷——蓝岩泉高尔夫球场，袭击的对象又是一男一女两个人。这次，男性受害者逃脱了死亡的命运，并且向警方提供了关于凶手特征的描述。此外，这起凶案还有许多奇怪的细节，这些细节也许能为查清凶手的身份提供进一步的线

索。这起凶案的受害者是22岁的达琳·费林（Darlene Ferrin）和19岁的迈克尔·马若（Michael Mageau）。达琳·费林已与迪安·费林结婚（迪安是她的第二任丈夫），并育有一个女儿。因此，我必须解释一下为什么她会和迈克尔出现在情人巷中。

根据警方的调查，在那天午夜前，达琳告诉家里的保姆她要为当天晚上正在举行的一个派对购买烟花。因此，她询问保姆能否留在家里照看她女儿直到凌晨0：15。也就是说，不管达琳打算出去干什么，她并不准备出门很长时间。事实上，当时购买烟花非常方便，整个城镇的多处售货摊处都有烟花卖。此后，达琳开车出门并且去迈克尔家里接上了迈克尔，当达琳把车开离迈克尔家时，迈克尔注意到有车在跟踪他们。于是，达琳加快了车速，后车紧追不舍。

后来，达琳撞上了高尔夫球场上的一段木头，被迫把车停了下来。此时，驱车追赶他们的那个人把车停在了达琳车辆的左后方，但又快速地再次启动车辆前进。达琳和迈克尔悬着的心放了下来。然而，安全只是暂时的，5分钟以后，那辆车又开了回来，再次停在先前的位置，并且车灯一直亮着。该车司机将强光对准迈克尔和达琳的脸，然后打开车门，走下汽车，走向他们。此时，之前照向他们的光熄灭了。迈克尔以为这个人是警察，因此他和达琳开始掏钱包要拿出证件。然而，这个陌生人走到车的副驾驶位一侧，再次用手电筒照了照迈克尔的脸，随后开枪射击。凶手的子弹打中了迈克尔，但是达琳受的枪伤更重，她一共身中9枪。接着，凶手回到自己车中，这时迈克尔清楚地看到了凶手的样子。但是凶手再次回到达琳的车辆旁边，并向两名受害者分别又开了两枪。

高尔夫球场的守夜人在零点左右听到了枪击声并且报了警，但是警方并没有把他的报告当回事，而是认为他听到的只是7月4日国庆日烟花燃放的声音。不久以后，3名青少年发现了达琳和迈克尔，其中一名打电话报了警，此时警方才意识到他们之前接到高尔夫球场守夜人的报案却没有立即行动是一个非常严重的错误。警方赶到现场时，凶手已经逃

之夭夭，还好他们尚有时间挽救迈克尔的生命。

虽然当时已是炎热的7月，迈克尔当时却穿着“三条裤子、三件毛衣、一件长袖带扣子的衬衣，以及一件T恤衫”。[注]有些作者认为迈克尔的穿着存在疑点，但是事实上关于迈克尔穿着的解释是非常简单的。迈克尔身高6英尺2英寸（约1.89米），并且身材非常瘦，他对这一点异常敏感，因此总是习惯多穿衣服以使自己看上去更结实一些。

由于在第二起案件中迈克尔没有被凶手杀死，而在第一起案件中贝蒂和戴维双双死亡，所以关于第二起枪击案的细节要比第一起多得多。然而，在迈克尔讲述的关于凶手如何开车追赶他们车辆的故事中却存在一些疑点。当然，如果一个人被发现与一名已婚女性一起待在情人巷里，那么当他解释自己出现在此地的原因时，编造一些细节也是可以理解的。事实上，在迈克尔叙述当晚的事件时，他的证词中出现了多处不一致的地方。然而，根据达琳从自己家开往迈克尔家的车速，以及从迈克尔家开往案发地点的车速来判断，他们确实有可能是在被人追赶。此外，当警方发现达琳的车辆时，汽车发动机并没有熄灭，车子处在低挡位，并且手刹也没有被拉上，这些情况都与迈克尔声称车辆因为撞上了一截木头而无法前进的证词相吻合。

但是，我还是必须解释当晚事件中另一处不合理的地方。达琳告诉保姆，她要出门去买烟花，然而在她死亡的时候，她的钱包里一共只有13美分。当然，对于这种情况也有一种很简单的解释：达琳开车接上了迈克尔，因此可能她认为迈克尔会帮她付买烟花的钱。

根据警方的调查，虽然达琳已经与迪安结婚，但她仍同时与若干男性约会，这些男性中甚至还包括当地治安办公室的一名警员。因此，婚外恋导致的嫉妒情杀可能是一种合理的凶杀动机。从这个方向考虑，可以拉出一份很长的嫌疑人名单。但是，接下来，一通电话从某一方面来讲把事情搞得更复杂了。案发当天凌晨0：40的时候（达琳被宣告死亡的仅仅两分钟之后），瓦列霍警察局的交换机接到了一通电话。在这通电话中，一名男子做了如下的声明：

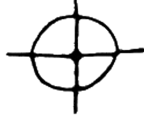
“我想要报告一起双重谋杀。如果你从哥伦布路向东往公共公园方向走一英里，你会在一辆棕色的车中找到两个孩子。他们是被一把9毫米鲁格尔手枪杀死的。去年的那些孩子也是我杀的。再见。”(注)

这段电话当时被录了下来，但是这段录音在1986年之前的某个时间被警方丢失了，因此，现在只有当年听过这段电话的人可以作为这通电话的人证。

根据警方对这通电话的追踪调查，这通电话是从瓦列霍治安办公室门口的一个公用电话打来的。由于在这通电话打进警察局的时候，只有少数几名警员知道这起谋杀，并且打电话的人提到了关于9毫米手枪的细节，所以警方认为这通电话确实是凶手打来的。

在凶杀案发生后不到一小时的时间内，有一名“呼吸沉重”的人连续给达琳的3名亲属打了电话。这一情况显示，凶手应该认识她。事后，达琳的一位朋友表示，曾听达琳说她认识此案的前两名受害者。此外，还有人证明达琳生前曾说自己目击到一个人谋杀了另一个人，而这名凶手显然是她非常害怕的一个人。根据多名认识达琳的人所述，很多事件都显示她似乎知道某起罪案的有关事情，然而警方始终未能找出这一犯罪事件的具体情况。在达琳死后，她的丈夫在她手中找到了一个奇怪的黄色信封。达琳的丈夫看到在信封上有“hacked（劈砍）”“stuck（困住）”“testified（作证）”“seen（看见）”几个单词，并且还有以下几个不完整的单词：“acrqu”、“acci”、“calc”和“icio”，“on”“by”“at”这几个单词被画上了圈。信封上还写有“highly”，但是又被划掉了。信封的背面写着一家餐馆的电话，这家餐馆的名字是“埃德先生免下车餐馆”(注)。

第一段密码



1969年7月31日，公众再次听到了凶手的消息。《旧金山纪事报》（*San Francisco Chronicle*）、《旧金山观察者报》（*San Francisco Examiner*）和《瓦列霍时报–先驱报》（*Vallejo Times-Herald*）三份报纸分别收到了自称是凶手的信件。我把凶手写给《旧金山纪事报》的信抄录如下。在这几封信中，凶手再次给出了公众不知道的信息，以证实自己确实是凶手本人，这和之前警方接到的电话的性质一致。这封信译文如下（原文中有一些拼写错误）：

亲爱的编辑，

我是去年圣诞节赫尔曼湖两名青少年遇害案的凶手，也是7月4日在瓦列霍高尔夫球场附近杀死那名女孩的凶手。为了证明确实是我杀了他们，我将在下面列出一些只有我和警方才知道的事实。

圣诞节案

1 子弹的牌子 超级X

2 共开了10枪

3 男孩仰卧，脚朝向车的方向

4 女孩右侧卧，脚朝西

7月4日案

1 女孩穿着有图案的宽松长裤

2 男孩的膝盖也中了枪

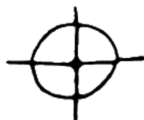
3 子弹的牌子是“西方”牌

完毕

以上是第一页的内容，在第二页上凶手继续写道：

随信附上一段密码，密码的另外两个部分我已分别寄给《瓦列霍时报－先驱报》和《旧金山观察者报》。我希望这段密码可以登在报纸的头版上。在这段密码中藏有我的身份。如果你在1969年8月1日星期五的下午前没有把这段密码登在报纸上，我将在星期五晚上展开疯狂的杀戮。如果这段密码不登出来，那么我整个周末都会四处巡游，杀掉夜里独处的人，然后继续杀人，直到我在周末杀够为止。

凶手用以下这个符号代替了签名：



对于这个神秘符号的含义，专业的警方调查人员和业余的侦探爱好者做出了各种各样的解读。看到这个符号，你会想到什么？在本章接下来的内容中，我会和读者一起讨论关于这个符号的几种可能性。

另外两份报纸也收到了类似的信件。这三封来自凶手的信分别附有一段不同的密码，详见图4–1至图4–3。(注)

图4-1 发给《瓦列霍时报-先驱报》的密码

图4-2 发给《旧金山纪事报》的密码



图4-3 发给《旧金山观察者报》的密码

如果不进行大量的分析工作，我们没有办法直接判断这3段密码究竟是3条独立的信息，还是应该结合在一起组成一段完整的信息。但是非常清楚的一点是，这些密码并不是MASC密码。这些密码中一共有54种不同的符号，只要简单地对这些符号进行计数，就可以清楚地看出加密方式不是MASC密码。如果凶手的密码中一共有36个符号，那么这36个符号可能代表英文中的26个字母和10个数字（0到9）。但是，由于这3段密码中总共包含54种不同的符号，因此多出的18种符号无法解释。也许，在这多出的18种符号中有一些是标点符号，比如句号、问号、逗号、撇等。虽然标点符号确实也可以有很多种，但是凶手似乎不太可能在这么短的信中使用这么多种不同的标点符号，因此54种不同的密码符号看起来似乎有些太多了。

54这个数对于MASC密码而言太多了，但是如果认为这些符号表示的是字母对、音节，或者单词的话，54这个数又太少了。表面来看，凶手似乎使用了一种提高MASC密码破译难度的最基本的方法，也就是用多个符号表示最常见的字母。比如，我们可以让R、M、T，以及加号都表示字母E。虽然这种方法非常简单，但是经过这一步骤之后，MASC密码的破译难度确实会显著提高。在这种方法中，表示字母的符

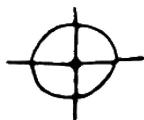
号被称为“同音字母”（homophones），而这种加密方式被称为“同音字母密码”。“同音字母密码”的加密方式最早可以被追溯到1412年，因此从密码学的角度来看，凶手并没有做出全新的突破。

在破解MASC密码的时候，我们手中最有力的两种工具是概率统计和单词规律研究，然而对于同音字母密码而言，上述两种武器都没有用武之地。此外，由于上文中提到的这封信件中包含不少拼错的单词，所以加密的信息中也很有可能会出现单词拼错的情况，这就给我们的破译工作带来了另外一重困难。

从另一个方面来看，这三段密码有一个非常有趣的特点，那就是：除了C以外，字母表上所有字母都出现了。其中的若干字母还以多种方式出现（比如倒着的，或者是左右反向的）。在这三段密码中我们有一个反向的C，但却没有正常的字母C。为什么会出现这种情况？

凶手每多写一封信，他不小心泄露线索的风险就越高，警方或许可以通过信里的线索发现凶手的身份，从而将他逮捕。基于这样的考虑，瓦列霍市的警察局局长杰克·E.施蒂尔茨（Jack E.Stiltz）公开邀请信件的作者提供更多关于凶杀案的细节，来证明他就是凶手本人。凶手接受了警方的这一邀请。

1969年8月7日的信



凶手的下一封信有三页纸长。在这封信中，他首次将自己称为“黄道十二宫杀手”（the Zodiac）。

这封信全文翻译如下：

亲爱的编辑，

我是黄道十二宫杀手。

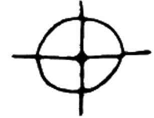
既然你们希望我详细讲述更多我在瓦列霍市欢度好时光的细节，我将非常高兴地向你们提供更多的资料。顺便问一下，警方还享受破译我的密码的感觉吗？如果不是的话，告诉他们，他们应该高兴起来，一旦他们破解出这个密码，他们就能够抓住我。

关于7月4日的谋杀：

我并没有打开车门，因为车窗已经被摇下来了。我开枪时，男孩本来坐在汽车的前座上。当我对着他的头开第一枪时，他突然向后仰去，因此我没有能够瞄准。男孩倒在了后座上，后座的地板把他的腿猛烈地弹回，所以我的子弹才会射中了他的膝盖。瓦列霍的报纸说我离开凶杀现场的时候轮胎吱吱作响，并且油门踩得很猛，事实并不是这样的。我是缓慢地离开现场的，这样就不会让其他人注意到我的车。告诉警方我的车是棕色的那个人是一个40~45岁的黑鬼，穿得相当破烂。他经过的时候，我正在电话亭里耍弄瓦列霍的警察。当我挂上电话的时候，那个可恶的东西突然开始响铃，这才使他注意到了我和我的汽车。

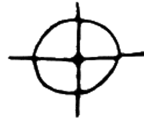
关于去年圣诞节的谋杀：

在这件凶杀案中，警方还不明白我为何能在黑暗中击中受害者的背部。虽然警方没有明确这么说，但是他们公布的信息暗示了这一点，因为警方宣称案发当夜灯光十分充足，还说我能在地平线上看到受害者的剪影。那简直是胡说，那个区域被高山和树木环绕着呢。实际上我是这样做的：我在枪筒上用胶带粘了一个笔形手电筒。如果你注意观察的话，当你把这种手电筒对着墙或者天花板的时候，你会发现光线的中心有一个圆形的黑点或者暗点，直径大概是3~6英寸。当你把这种手电筒用胶带粘在枪筒上时，子弹正好可以击中手电筒光线中心的黑点。因此我只需要像洒水一样地到处放枪就行了，根本用不上瞄准器。我的信息没有上头版，对此我很不高兴。



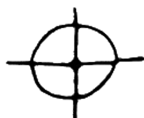
凶手在信中写道："顺便问一下，警方还享受破译我的密码的感觉吗？如果不是的话，告诉他们，他们应该高兴起来，一旦他们破解出这个密码，他们就能够抓住我。"在写下这句话的时候，凶手显然没有意识到，他的密码已经被破译了。

快速破解



凶手的这段密码被提交给了国家安全局（NSA）、中央情报局（CIA），以及联邦调查局（FBI），然而，最终解开这段密码的却是两位在报纸上看到这段密码的业余密码爱好者。唐纳德·哈登（Donald Harden）是一名高中历史和经济学老师，他在开始破译这段密码之后，他的妻子贝蒂·哈登（Bettye Harden）也加入了这项工作。贝蒂·哈登此前并没有任何密码破译方面的经验。接下来，我将详细介绍哈登夫妇破译这段密码的方法。当然，读者也可以暂时停止阅读下文，尝试自己解开这个密码。我要事先警告读者，这段密码是非常难以破解的！然而，如果你非常聪明，也许你可以用比哈登夫妇更短的时间解开这段密码。哈登夫妇解开这段密码只用了20个小时。

破译过程



唐纳德从小就对密码有兴趣，并且他也有密码学方面的书籍可以作为参考。然而，贝蒂却拥有两项对于破解密码而言极度宝贵的特质，那就是坚持不懈的毅力以及丰富的创造力。当唐纳德想要放弃的时候，贝蒂却不愿放弃，她拖着唐纳德继续回到密码破译的工作上去。最终，贝蒂想到了破解该密码最关键的一个方法，那就是揣摩罪犯的心理。创造这些密码的凶手显然希望得到公众的关注，否则他就不会写这些信了。一个如此以自我为中心的人很可能会用“I（我）”作为这封信的第一个字。此外，贝蒂还猜测，“KILL（杀人）”这个词会出现在信息中。她甚至进一步猜测，这条信息的第一句话可能是类似于“I LIKE KILLING”（我喜欢杀人）这样的句子。

这种站在创造者的角度去猜测他会在密码中使用什么样的单词或者词组的技巧曾无数次为破译者带来成功。甚至在第二次世界大战期间盟军破译纳粹恩尼格玛密码的时候，这个技巧也发挥了作用。密码破译专家把上述技巧与一些更加复杂的数学技巧，以及特殊设计的机器（“炸弹”机）相结合，取得了非常理想的效果。

在一段密文中寻找某个特定的词（比如“KILL”这个词），这一步骤被密码专家称作“可能词”，或者有时也称为“可能词搜索”。这种可能词也被称为“照抄词”（crib），而搜索可能词的过程被称为“照抄”（cribbing）(注)。“照抄”这一过程给哈登夫妇带来了丰硕的成果。

“KILL”这个单词是以两个L字母结尾的，如果是MASC密码，只要找到连续出现的两个同样的密码符号就行了。然而，我们研究的这个密码可能会用两种或更多种符号来表示字母L，因此我们就必须更加灵活地来处理这个问题。幸运的是，在这个密码中，确实有连续出现两次的

符号。“■■”这对符号两次出现在了密码中（在两个不同的密码片段中），此外，“■■”这对符号也出现了一次。而且我们还看到“R R”在密码中出现了一次。在正常的英语中，有些字母（比如字母Q）从来不会连续出现两次。而“L”是所有英文字母中连续两次重复出现的概率最高的一个字母。因此，我们有理由假设“■■”代表的是“LL”。但是，我必须再次提醒读者，这套密码还可能用其他符号来表示字母L。不管怎么样，如果我们假设“■■”表示“LL”，并且假设含有“■■”的单词是“KILL”，那我们就可以根据这一判断进行相应的代换：/△■■（K I L L），因此我们可以暂时假设“/”表示字母K，而“△”表示字母I。

需要强调的一点是，我们也可以对另一处“■■”做同样的替换，但是这么做就会将我们引上歧途。在破译密码的过程中，我们会遇到很多错误的线索。在我们沿着一个错误的方向前进以后，最终我们会清楚地认识到自己犯了错误，此时就必须回到原点重新寻找方向。但讨论所有这些错误的线索，并且描述回到原点重新寻找方向的过程，会让我们的分析变得极为冗长。因此，在描述密码破译过程的时候，作者通常只会向读者展示最终得到正确结果的那条路径。

现在，我们假定已经知道表示字母K、I，以及L的几种符号，在整段密码中，可以多次找到这些符号并将它们代入。完成了这个代入的步骤以后，其中一段密码的第一行就变成了

△■ P / Z / U B■ K O R ᴧ 9 X ᴧ B。

当哈登夫妇看到这行句子的时候，他们意识到这段密码的第一句话是“I LIKE KILLING（我喜欢杀人）”，这正和贝蒂的猜测一模一样！这一发现不仅显示出三段密码中哪段是第一段，并且还让哈登夫妇成功地找到了以下这些字母和符号之间的对应关系：“P”“U”“K”代表字母I，“Z”代表字母E，“B”代表字母L，“O”代表N，“R”代表字母G。

在破译密码的过程中，常常会出现这样的情况：破译者一旦做出了一个重要突破，剩下内容的破译速度就会大大提高。读者可以在此停止阅读，并且尝试自己完成剩下的破译工作。但是读者必须记住，在这段

密码中很可能会出现一些拼错的单词。我将破译后的完整明文摘录于后文。

在破译这段密码的过程中，最关键的一步是找到代表字母“LL”的符号。一开始，有三组符号可能代表“LL”，这三组符号分列是“■■”“■■”和“R R”。其中，“■■”代表“LL”的可能性最高，因为它在密码中出现了两次，而其他两组符号分别只出现过一次。但是，当这段密码被完全破解以后，我们发现其实“■■”和“■■”都代表字母“LL”。而“R R”代表的是字母“GG”。

破译黄道十二宫杀手密码的过程确实如我们所料，相当复杂，因为凶手的原文中出现了若干错误。

破译后的明文译文如下：

> 我喜欢杀人，因为杀人太有趣了。杀人比在森林中猎杀野味更加有趣，因为人才是世界上最危险的动物。杀戮给我带来了最为震撼的经验，那种感觉甚至比跟女孩做爱还要好。而且最好的一点是，在我死后，我将在天堂中重生，而我杀掉的所有人都会成为我的奴隶。我不会告诉你们我的名字，因为知道了我的名字，你们就会试着拖慢我的脚步，甚至会完全阻止我为自己身后积累奴隶的行为。EBEORIETEMETHHPITI

多家报纸刊登了这段破解后的明文的不同版本——有的修正了原文中的拼写错误，有的反而引入了新的拼写错误。上面这段破译后的信息中没有包含字母J、Q和Z。这一点也许可以解释为什么杀手密码的密文中没有出现“C”。也许“C”代表J、Q，或者Z，所以在这段信息中不需要用到它。

在这段信息的末尾出现了“EBEORIETEMETHHPITI”这串字母。许多人都试图从这段字母中破解出一个名字，似乎这样做就可以揭示出凶手的身份。(注)

然而，所有这些尝试都不可能是正确的，因为在已经被破译的明文中凶手清楚地表明了："我不会告诉你们我的名字。"唐纳德·哈登认为，这段字母可能没有什么意义，只是为了把密码所在的长方形的最后一段填满而已。

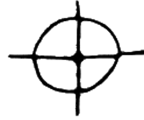
虽然哈登夫妇在1969年8月4日就已经破解了这个密码，但是他们却没有办法立即说服其他人相信他们已经破解成功。因此，这段密码的明文直到1969年8月12日才被发表在报纸上。

直到上述这段明文被发表以后，一位给《旧金山纪事报》画政治漫画的漫画家罗伯特·格雷史密斯（Robert Graysmith，此人也对黄道十二宫杀手案极有兴趣）才发现这些信件的信封上有一条线索，已经提示了这三段密码的先后顺序。装有第一段密码、第二段密码、第三段密码的信封上分别贴了两张邮票、三张邮票，以及四张邮票。

奇怪的是，在哈登夫妇的破译结果发表之前，就有人匿名将这份密码的密钥寄给了瓦列霍市警察局的侦缉探长约翰·林奇（John Lynch）。这封信是来自凶手本人吗？还是来自一位胆小的"热心市民"？这封信的署名确实是"热心市民"，也许他这么做是因为不希望吸引凶手的注意。

每条确认来自凶手的信息都有其潜在的价值。读者恐怕已经猜到，如果黄道十二宫杀手案中的所有密码都被破解的话，我就不会把这个案子写在本书中了。也许，我在本书中抄录的某一封信会给某位读者一些心理上的启发，并帮助这位读者最终破解这些目前尚未被破解的杀手密码。这样的事情会发生在不久的将来吗？

贝里耶萨湖案



1969年9月27日，星期六，黄道十二宫杀手又犯下了另一起罪案。这次的凶杀案发生在白天，但仍然在一个比较偏僻的地点。

这一天下午4点，20岁的布赖恩·哈特内尔（Bryan Hartnell）和22岁的塞西莉亚·谢珀德（Cecilia Sheperd）驾车来到了瓦列霍市以北36英里处的贝里耶萨湖。布赖恩和塞西莉亚在湖中伸出的半岛上享受了一顿野餐，然后悲剧便降临在他们身上。

凶手接近这对年轻人的时候，和之前一样带着一把枪。但不同的是，这次凶手还带了一把有木鞘的大刀，并且把这把刀挂在他的腰带上。此外，凶手还拿着绳索，并穿着特殊的服饰。这套服饰包括一个黑色的头罩，戴着头罩的凶手看起来有点儿像所谓的“行刑者”。某本杂志在封面上复原了穿着特殊服饰的凶手的形象，见图4–4。正如图中展示的那样，凶手戴的头罩一直延伸到胸部，上面还带有凶手在写给报纸的信件中用作签名的标志。但是，该杂志对凶手形象的复原图并不完全准确。事实上，凶手戴的头罩在嘴部有一个裂缝，此外凶手在头罩之外还戴了一副用夹子夹住的太阳镜，因此他的眼睛也被挡住了。

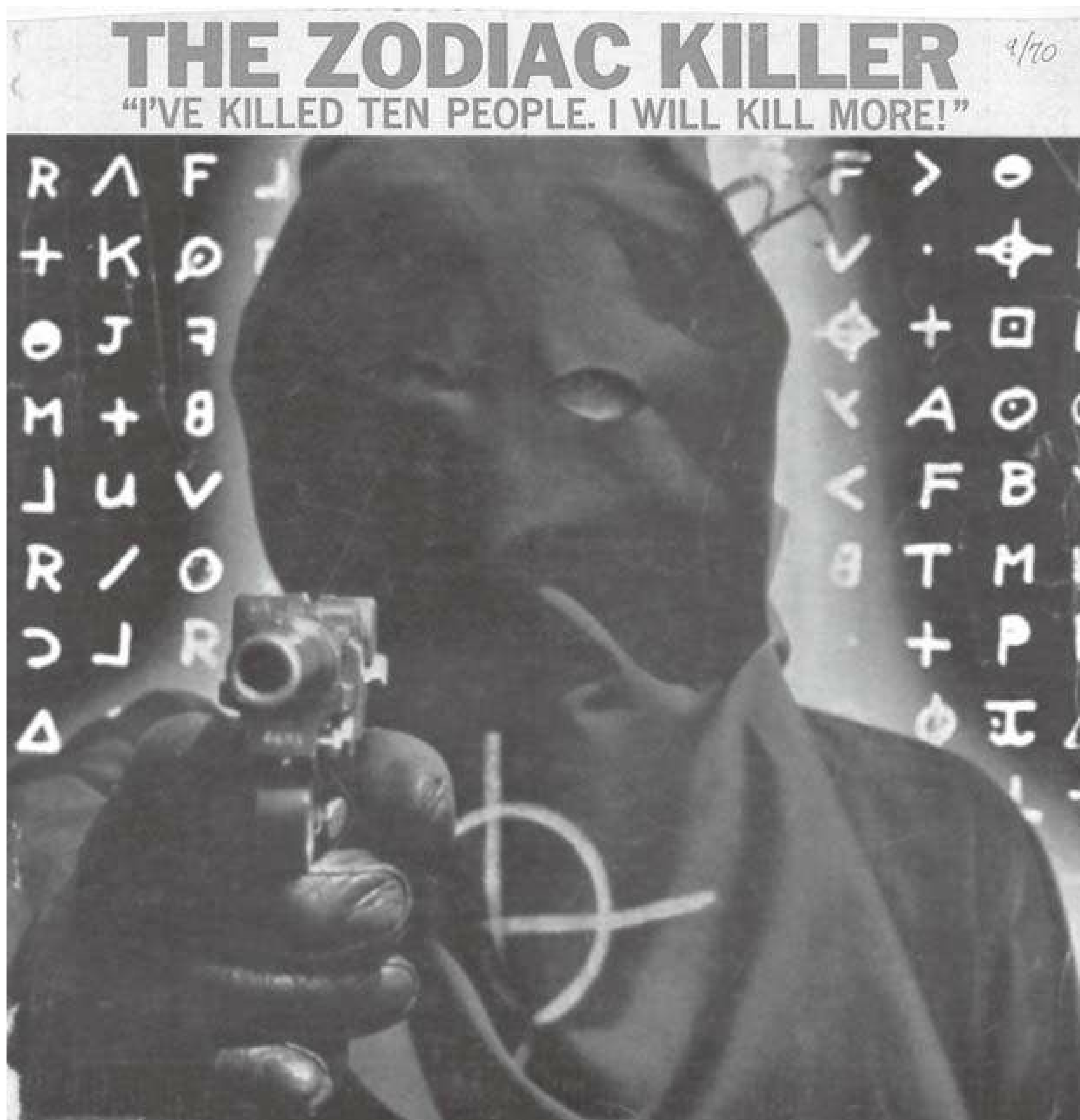


图4-4 穿着特殊服饰的凶手形象的复原图

凶手拿出一把半自动手枪，并对两名受害者说："我要你们的钱和车钥匙。我要把你们的车开到墨西哥去。"注布赖恩把身上所有的钱（不到一美元）以及车钥匙都交给了凶手。虽然这名持枪歹徒看起来精神不太正常，但是布赖恩以为自己只是遭到了抢劫，所以他全程都非常配合。凶手把布赖恩递过来的钱和车钥匙放进了自己的口袋，然后收起

了手枪。接着，凶手告诉这两个年轻人：“我是蒙大拿州迪尔洛奇监狱的一名逃犯。我杀了那里的一个监狱看守。我一无所有，手里只有一辆偷来的车，没什么可失去的。”然后，凶手又说了一些话，并且拿出了手上的绳子。那条绳子是一种空心的塑料晾衣绳，绳子已经被剪成三英尺的长度。凶手对两名年轻人说：“脸朝下趴在地上。我得把你们绑起来。”[注]布赖恩稍微跟凶手争论了一下，但最终还是选择了服从。凶手让塞西莉亚把布赖恩绑起来，于是塞西莉亚就把布赖恩松松地绑了起来。接着凶手把塞西莉亚也绑了起来，并且重新把布赖恩身上的绳子绑得更紧。随着天色渐渐变黑，凶手和这对年轻人又进行了一些冷静的对话。最后，凶手说道：“我要用刀子捅死你们。”[注]

一开始，凶手先用刀捅向布赖恩的后背。接着他转向塞西莉亚，开始用刀捅她。在塞西莉亚挣扎的过程中，她滚到一边变成了脸朝上的姿势，因此她的身体正面也有多处刀伤。布赖恩假装已经死亡。于是凶手把从这两位年轻人身上抢来的钱和车钥匙都扔到了毛毯上，然后离开了现场。这一举动说明，凶手这次行凶并不是像他之前所说的那样，为了钱或者交通工具。在离开凶杀现场的过程中，凶手停下来用一支黑色的毡制粗头笔在布赖恩的汽车门上写下了一段信息。这段信息以黄道十二宫杀手在信件中所用的签名符号（一个圆圈和一对互相垂直的线条，两条线在圆心处相交）为开头。画完这个符号以后，凶手又留下了一些文字和几个日期。凶手留在汽车门上的这条信息参见图4–5。

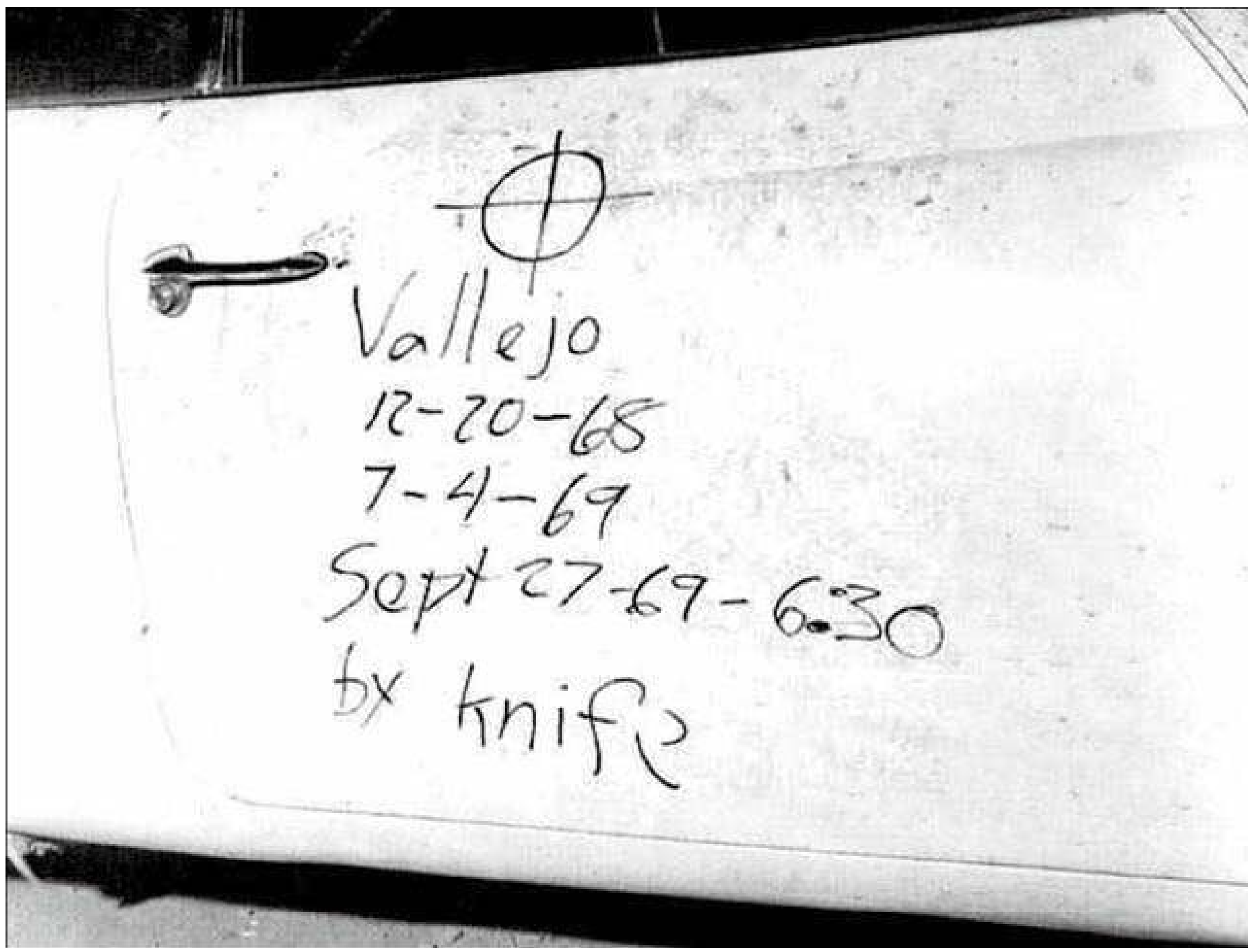


图4-5 凶手留在车门上的一条信息

车门上的这条信息是第一条把这件凶案和黄道十二宫杀手联系起来的线索。由于这件凶案的许多细节都与黄道十二宫杀手之前犯下的案件不符（犯案时间是白天而不是晚上，凶手用的凶器是刀而不是枪），所以如果没有车门上的这条信息，警方很可能不会把这起案件和之前的两起案件联系起来。

令人惊奇的是，在凶手离开凶案现场后，布赖恩和塞西莉亚都还活着。这两位年轻人甚至成功地挣脱了绳索，但是他们没有足够的体力爬进汽车。后来，两名渔夫听见了受害者的呻吟声，两位受害者这才得救。

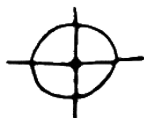
车门上的信息并不是唯一一条将这起凶案和黄道十二宫杀手联系起

来的线索。案发以后，黄道十二宫杀手在当晚的7：40给纳帕警察局打了电话，电话的内容如下：

> “我要报告一起谋杀案——不，是一起双重谋杀案。案发地点是公园总部以北两英里处，受害者在一辆白色大众卡曼吉亚汽车中。我就是杀人凶手。”㊟

警方追踪了这通电话的来源，并且在凶手使用过的公用电话上取得了一个掌印。凶手并不知道受害者获得了渔夫的救助。两名受害者都被送往了医院，但是只有布赖恩活了下来。塞西莉亚身中24刀，于次日下午3：45死亡。

旧金山市中心案



回顾起来，黄道十二宫杀手制造了一系列连环凶杀案。在第一起案件中，凶手杀死了一名青少年男性和一名青少年女性。然而，在接下来的两起凶案中，虽然凶手认为自己杀死了一对情侣，但是这两起案件里都只有女方毙命。证据清楚地显示，两名男性受害者之所以能够生还，是因为凶手对女性受害者的攻击强度远远高于男性。也许这使得凶手觉得有必要证明一些事情。因此，在接下来的一起凶案中，凶手选择了一名男性作为袭击目标。在贝里耶萨湖案件发生后两星期，就发生了接下来的一起凶案。

1969年10月11日星期六，黄道十二宫杀手出现在旧金山市中心。凶手拦下了一辆出租车，并且让司机保罗·斯泰恩（Paul Stine）驱车前往

华盛顿街和枫叶街的交叉口。这个地点位于一片名为“普雷西迪奥高地”的住宅区中。当出租车到达指定地点时，车前灯照亮的区域中恰好有一个人在遛狗。于是，凶手要求司机“再向前开一个街区”。[注]在华盛顿街和樱桃街的交叉口，凶手拿出一把9毫米手枪对准了保罗的头，并用另一只手臂勒住了保罗的脖子，随后扣动了扳机。然后，凶手从车后座下车，并打开出租车的前门坐到了副驾驶位上。在副驾驶位上，凶手把保罗被枪击过的头颅放在自己的膝盖上，并拿走了保罗的钱包。

保罗是旧金山大学英语系的博士生，他遇害时只有29岁。此前，所有遭到黄道十二宫杀手攻击的受害者都是学生，只不过年龄有所不同。这可能是因为黄道十二宫杀手喜欢在情人巷伏击受害者，而在这种地点最容易遇到的就是年轻人。和此前遇害的达琳一样，保罗也是一名已婚人士。

在此次凶杀案发生后的几分钟内，杀手差点儿就被当场抓住。在案发前，凶手要求保罗向前多开了一个街区，他这么做似乎是为了避开潜在的目击证人，然而，这次他还是被看见了。凶手杀人后坐在出租车的副驾驶位上，把保罗的头颅放在自己的膝盖上，并拿走了保罗的钱包，然后又擦拭了出租车的内部。在这个过程中，一名14岁的女孩在出租车前方看见了凶手。这位女孩立刻叫来了她的两个兄弟，于是这两位兄弟也成了本案的目击证人。在凶手走出出租车以后，这几个孩子还看到凶手擦拭了出租车的外部。然后，凶手就关上车门走开了。

当天晚上9：58，上述几位目击证人打电话报警，他们对凶手的描述是“一位穿着深色夹克的白人男性”。然而，接电话的警员却犯了错误，他们记下的信息变成了“黑人成年男性”。[注]几分钟后，巡逻警员唐纳德·福克（Donald Fouke）和埃里克·泽尔姆斯（Eric Zelms）赶到了现场，他们看见一位白人男性在街上行走，行走方向和目击证人汇报的凶手行走方向一致。于是，这两名警员向这名白人男性大声呼喊，并询问他是否曾经看到什么情况。这名白人男性对警员的问话做出了回应，他声称看到一个人挥舞着枪向东跑向华盛顿街。于是，福克和泽尔姆斯根

据这条错误的线索向东走去，而这名白人男性之后再也没有进入警员的视线。由于这两名警员距离该白人男性较远，并且这名白人男性穿着深色的衣服，再加上夜色和阴影的影响，警员并没有看清凶手当时身上的大片血迹。直到当天夜里的晚些时候，警方才掌握了目击证人对凶手外貌的准确描述。警方还根据这几个目击证人的描述对凶手的外形进行了素描。

福克和泽尔姆斯后来也认识到自己所犯的错误，两人最终向上级汇报，称他们认为之前询问过的那名白人男子很可能就是凶手本人。对于这两名警员来说，承认自己的错误、说出实情，并补充他们能回忆起来的凶手特征描述是需要相当大的勇气的。仅仅几个月之后，即1970年元旦，泽尔姆斯就在执行任务时不幸因公殉职，当时他只有22岁。

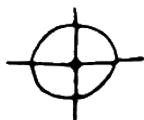
然而，当福克和泽尔姆斯的上级处理这两名警员提交的新信息时，他们却没有表现出和这两名警员同样的勇气。警方对凶手的外貌进行了新的素描，但却从来没有向公众解释这一行为的原因。并且，警局官方一直否认有任何警官看见过凶手。

现在回顾起来，我们已经知道，凶手声称只要解开那三段密码就会找出他的身份是在说谎。警方声称他们在斯泰恩被杀之后没有发现凶手，警方显然也在说谎。而此前目击了凶案发生过程的迈克尔·马若的证词中也有一些前后矛盾的情况，因此他的证词中也可能包含谎言。那么，在黄道十二宫凶手的其他案件中，是否也出现过未被发现的谎言呢？当每件事情都存在疑问时，要想获知真相就变得更加困难了。

在与警方打过照面以后，凶手还被其他目击证人看到过。据目击证人称，凶手走进了“普雷西迪奥高地的茂密树林中”。[注]警方出动警犬对公园进行了搜索，但是也许为时已晚。警方在搜索中没有发现任何人。

然而，警方手中还掌握着关于凶手的另外一条线索：在斯泰恩的出租车上发现了一个右手的血掌印。警方决定对这条线索进行保密。调查对比显示，这枚血掌印并不是死者斯泰恩的。

1969年10月13日的信



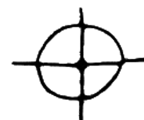
与之前的几起谋杀案一样，在此案发生以后，凶手给《旧金山纪事报》寄去了一封信。由于信中提供了只有凶手才知道的细节，所以可以非常确定这封信的作者就是凶手本人。凶手还随信寄来了一块“3英寸乘以5英寸大小的灰白相间的布，这块布不是被刀割下来的，而是整齐地撕扯下来的，布上溅有血迹”。(注)凶手寄来的布与死者保罗·斯泰恩的衬衣上缺失的一块布吻合。凶手在信中写道：

我是黄道十二宫杀手。

我是昨晚在华盛顿街和枫叶街交叉处杀死那名出租车司机的凶手。为了证明这一点，随信附上死者衬衣上的一块带血的布。北湾地区的那些人也是我杀死的。

如果昨天晚上旧金山的警方好好地对公园进行搜索的话，他们本可以抓住我的。然而，他们却只是骑着摩托车在路上飞驰，仿佛在比谁发出的噪声更响。那些开车的警察应该停好他们的车，然后坐在那里静静地等待我从树林中走出来。

上学的孩子是很好的谋杀目标，我想我某一天早晨会袭击一辆校车。只要射坏校车的前轮，就可以等着校车上的孩子从车里蹦蹦跳跳地走出来了。



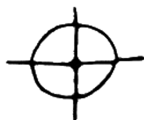
从之前的信件中我们知道，凶手并不吝于在给警方的信件中撒谎。

然而，警方不敢把凶手关于袭击校车的威胁当作虚张声势，因为凶手也有可能真的执行信中的计划，这其中的巨大风险是警方无法承担的。于是，警方把这一情况通报给了该区域的学校官员，而学校官员对此的回应是："对于这样一个威胁，我们再怎么小心提防都不为过。"㊟

为了防止校车受到狙击手的攻击，纳帕谷联合学区在每一辆校车上安排了一名额外的保安人员，70个警察分队全副武装地在校车上执行安保任务，另外一些警察则开着林业部门或者护林站的货运卡车跟在校车后面进行保护。在旧金山市内，便衣警察开着没有警察标志的车辆负责跟踪保护校车，此外还有超过100辆警车参加了该项任务。警方甚至还出动了空中巡逻机来应对凶手的威胁。

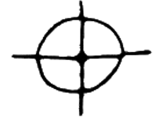
也许上述保护工作中的某一项或者某几项导致凶手无法实施他在信中说到的袭击，也许凶手从来没有真的打算袭击校车，我们永远无法知道真相。但我们知道的是，湾区的孩子们安然无恙，没有发生任何针对校车的袭击事件。然而，凶手的信却还在继续寄来。

1969年11月8日的信



凶手在11月寄出的第一封信写在了一张贺卡上。在信中凶手写道：

我是黄道十二宫杀手。我想，在你们再次收到坏消息之前，你们可以开怀大笑。在最近的一段时间内，你们不会收到新的坏消息。另：你们可以把这段新的密码刊登在头版上吗？当别人忽略我的时候，我觉得特别孤独，这使我又想做我爱做的那件事了！



七月 八月 九月 十月=7

截至写这封信的时候，黄道十二宫杀手共攻击过7名受害者，其中两名生还，5名死亡。那么这封信里提到的7这个数字是指7人受到攻击，还是指7人被杀呢？如果信中的7指的是有7人被杀的话，我们并不知道剩下的两名受害人是谁。截至当年8月，该地区唯一尚未破获的凶杀案中有两名少女遇害。然而，在案发将近两年后，这起本与黄道十二宫连环凶杀案无关的案件看起来也有了关联。

如果说黄道十二宫杀手写这封信的目的不是承认某些尚未与他联系起来的谋杀案是自己所为，那他为什么要在信中提到8月呢？也许，他是在报纸上读到了8月份发生的杀死两名少女的案件，并且认为自己可以通过写信的方式偷取此案的“功劳”。然而，如果这封信目的是要承认一件已经发生了几个月的谋杀，那么凶手为什么要在信中说“在最近的一段时间内，你们不会收到新的坏消息”呢？在这封信中，凶手没有提供任何证据或者公众不知道的内部信息，这一点和此前的信件相当不同。关于这些问题，事后迈克尔·D.凯莱赫（Michael D.Kelleher）和戴维·范纳伊斯（David van Nuys）[注]在他们所著的书《我是黄道十二宫杀手：深入连环杀手的内心》（*This Is the Zodiac Speaking: Into the Mind of a Serial Killer*）中提出了一种比较令人信服的理论。他们认为：由于在保罗·斯泰恩的谋杀案中黄道十二宫杀手差点儿落入警方的手中，因此在斯泰恩案后，凶手再也没有制造过新的凶杀案。凶手只是继续写信，号称受害者的数目在继续上升而已。

凶手寄来的这张卡片还附有一段新密码。这段密码通常被称为340密码，因为这段密码中包括340个符号。

这段密码看起来和之前哈登夫妇破解的三段密码一样，也是一种“同音字母密码”。然而，这次哈登夫妇没有能够破解出这段密码。事

实上，没有任何人成功地找到了这段密码的答案。如果把之前的三段密码中所使用的字母替换法则代入这段新密码，只会得到一些毫无意义的文字。或许黄道十二宫杀手写的本来就是毫无意义的胡言乱语呢？凶手是否故意寄来一段其实没有任何意义的密码，来跟警方开玩笑？根据格雷史密斯的说法："国家安全局认为，这段密码中肯定包含某种信息。"[注]除了这段引自官方权威机构的结论以外，格雷史密斯还提出了另外一个有信服力的证据，来证明这段密码中确实含有某种信息：在这段密码中，第6行第12列中的字符被涂改和修正过。如果凶手只是在这段密码中随便写出一些随机字符的话，又为什么要对其中的一个字符进行涂改和修正呢？写什么字符不是都一样吗？

在格雷史密斯所著的书《黄道十二宫》（*Zodiac*）中，他提出了对340密码的一种解法，但是这种解法并没有被广泛接受。以下是格雷史密斯对340密码的解答的译文，请读者自行判断它是否合理。[注]

赫布·凯恩[注]：

我也让他们如在地狱。

打碎这些谎言。侦探

应该能看出一个名字

在杀手的电影之下。一些药丸

游戏。原谅我接受

打碎我。狗屎。

这些愚蠢的人应该遇见

杀手。请询问LUNBLAD。

灵魂在H LSD UL

清澈的湖水。看着我

吞下一粒药丸。混蛋。我

栽赃给A.H.先生。打电话B湖

所有的奴隶都因为LSD

会偷走任何一个奴隶

我是否应该砍托斯基？

猪圈的买卖

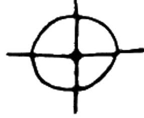
第八个灵魂被杀死。

在我看来，上面这段文字的行文实在太不自然了，因此这不可能是340密码的正确解法。事实上，格雷史密斯已经对这段明文做过一些灵活的处理，这才让这段文字看起来勉强能够读懂。格雷史密斯不仅进行了替换，还改变了一些字母的顺序。也就是说，他进行了一定程度的“重排”，这种重排是在单词层面上进行的（在一个单词的范围内可以交换字母的顺序，但是不能在词与词之间交换字母）。在格雷史密斯的解法中，“Ɔ”这个符号没有任何意义，也就是说，这是一个空符。而“K”符号却既代表字母K，又代表字母S。

为了解开这段密码，警方向美国密码协会以及门萨俱乐部寻求帮助。门萨俱乐部的一位会员加雷思·佩恩（Gareth Penn）首次注意到了340密码的一个细节，那就是：在这段密码的结尾，出现了“Zodiac（黄道十二宫）”一词的变体，然后又跟着两个其他符号。这只是一个巧合吗？或者，这种现象会不会意味着信中的某些字母并没有被加密成其他字符，且在密码中确实存在一些换位重排的现象？

在这段（我个人认为）至今尚未破解的密码之后，凶手又寄来了另一封长信。

1969年11月9日的信



这次的信件又是寄到《旧金山纪事报》。在这封信中，凶手非常明确地提出，他已制造了7宗谋杀案，而不是仅仅对7名受害者进行过袭击。这封信的内容如下：

我是黄道十二宫杀手。截至10月底，我已经杀了7个人。警方一直在散播关于我的谎话，对于这一点我非常生气。因此我将改变我积累奴隶的方式。我将不再对任何人做任何事前的声明。当我进行谋杀时，这些谋杀看上去就像常规的抢劫、愤怒杀人，以及一些伪造的事故等。

警察永远抓不住我，因为我太聪明了。

1. 虽然警方公开了一些关于我的描述，但是只有在我做那件事情（指杀人）的时候，我才会那样打扮。在其他时候，我看起来完全不同。我不会告诉你们当我杀人的时候我进行了哪些伪装。

2. 虽然警方号称有我的指纹，但是到目前为止我事实上没有留下过任何指纹。当我杀人的时候，我的手指尖戴着透明的保护物。实际上，我在我的指尖上涂了两层飞机黏合剂——这么做不仅别人很难注意到，而且非常有效。

3. 我谋杀所用的工具都是在警方颁发禁令以前通过邮购的方式获得的。除了其中一件，是在其他州购得的。因此你们可以看到，警方手里根本没有什么破案的线索。也许你会问，为什么我要擦拭那辆出租车？事实上我在留下一些假线索，好让警方围着它团团转——用某些人的说法，这叫作给警方“派些活儿”，好让他们有得忙。我非常享受用针刺那些蓝猪的过程。你好蓝猪，我曾经躲在公园中——你们用救火车的声音来掩饰偷偷巡逻的警车。你们的警犬

从来没有靠近过我，与我的距离总是大于两个街区+它们往西边去了+当摩托车从南边开向西北方向的时候，只有两组人停下车，他们相距大约10分钟车程，而他们从我身边疾驰而去时离我最近的距离也只有150英尺。

又及：在我离开那辆出租车大约3分钟以后，两个警察犯了严重的错误。我正朝山下走向公园方向，警车停了下来+其中一个警察把我叫过去+问我是否在过去5~10分钟看到任何行为可疑或是奇怪的人+我说是的，有一个人跑过去，手里还挥舞着枪，于是这两个警察飞速地启动了汽车+他们朝着我指的方向，开向了转弯处+而我在一个半街区以外消失在了公园中，再也没有人看到我。

你们好啊，猪们，你们对自己犯下的大错不感到生气吗？

如果你们这些警察真的认为我会像我所声明的那样袭击校车的话，你们的脑袋都应该被子弹打上几个洞。

只要一袋硝酸铵肥料+1加仑烧炉子用的油，再在上面放上几袋碎石+点燃这玩意儿+就能炸掉几乎所有东西。

死亡机器已经造好了。我本想给你们寄去死亡机器的照片，但是你们太讨厌了，你们一定会追踪到冲洗照片的人+然后再追踪到我。所以我只能用语言描述我的杰作了。这种死亡机器最好的地方是，所有部件都可以在公共市场上买到，没有人会对买这些东西的人提出任何疑问。

1个电池钟——可以运转大概1年时间

1个光电开关

两个铜片弹簧

两个6伏汽车电池

1个手电筒灯泡+反光镜

1面镜子

两个18英寸黑色纸板管，里外都放上鞋油

（接下来是一整页关于“死亡机器”的图片）

我已经全面测试过上述系统。然而，你们不知道的是：这种死亡机器究竟已经放在你们面前，还是被我保存在地下室里以备后用。我想你们没有足够的人力来一直对路边进行搜索，寻找我的死亡机器。+即使给校车涂上别的外观+改变校车的行车路线也没有用，因为这种炸弹可以根据新的情况进行调整。

好好享受吧！！顺便说一声，要是你们敢吓唬我的话，场面可能会变得相当难看。

接下来，这封信中出现了一张图，见图4–6。你觉得这张图是什么意思呢？

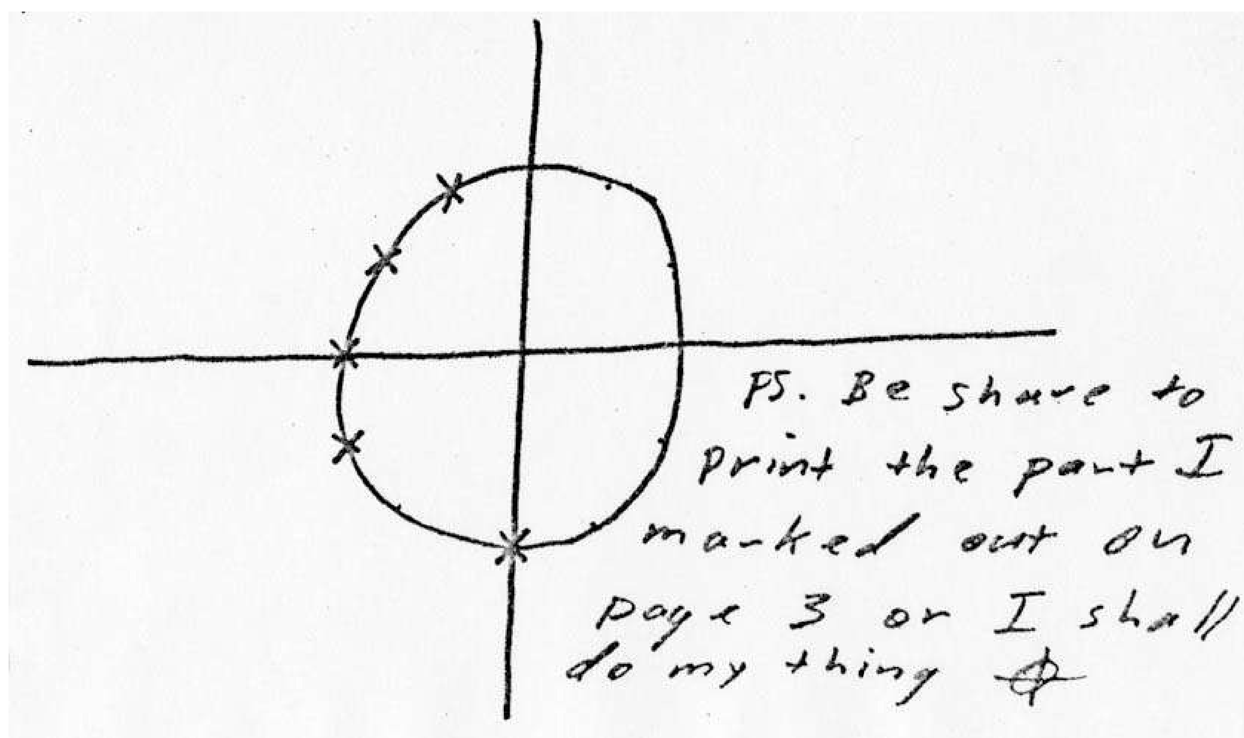


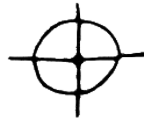
图4-6 来自凶手的一幅奇怪的图

警方相信，这张图表示某种日历，上面标出了凶杀发生的月份。凶手的这封信最终以一段附言结尾。

又及：一定要把我在第3页上标出的那部分刊登到报纸上，否则我就会做我爱做的那件事情。为了证明我就是黄道十二宫杀手，你们可以向瓦列霍警方询问我的电子枪瞄准器，那是我开始积累奴隶时使用的工具。

虽然凶手在这封信中提供了一些关于斯泰恩案的细节以及他逃脱的过程，但凶手并没有提出任何把自己和尚未受怀疑的凶杀案联系起来的证据。因此，凶手关于“我已经杀死了7个人”的声明是值得怀疑的。

1969年12月20日的信



黄道十二宫杀手的下一封信寄给了著名律师梅尔文·贝利（Melvin Belli）。我将这封信复制如下：

亲爱的梅尔文，

我是黄道十二宫杀手，我祝你圣诞节快乐。我有一事相求，请你帮助我。我没有办法自己去寻求帮助，因为我的内心不让我去寻求帮助。我觉得要控制住自己极其困难，我担心我会再次失去控制，并杀死我的第9个，甚至第10个受害者。请帮助我，我快要不行了。目前，孩子们还不会受到炸弹的攻击，因为装置炸弹需要做许多挖掘的工作，并且需要花费精力去调节触发机关才能调整好。但如果我等得太久了，我就会~~完全~~失去所有对自己的控制，并装好炸弹去杀人。请帮助我，时间长了，我就控制不住我自己了。

许多研究者都很关注这封信中的“Happy Christmass[注]（圣诞快乐）”，因为在美国，人们更习惯说“Merry Christmas”。抛开拼写的问题不谈，黄道十二宫杀手在这封信中的用语更像是英格兰人或者加拿大人。那么，黄道十二宫杀手会不会是一名英国人呢？

此前在1969年10月22日，一名自称是黄道十二宫杀手的人曾经致电奥克兰警察局表示，如果F.李·贝利（F.Lee Bailey）或者梅尔文·贝利能出现在七频道的脱口秀节目中，他想和他们对话。于是，梅尔文·贝利真的出现在了七频道的脱口秀节目中，并且与一名自称是黄道十二宫杀手的人通话了很久。然而，最后警方的追踪结果显示，这通电话来自一个精神病院。

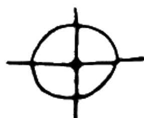
但最奇怪的地方是，上面展示的这封写给梅尔文的信中附有一片来自保罗·斯泰恩血衣上的布片。难道说事情真有这么巧，一个住在精神病院的人和真正的黄道十二宫杀手都想要和梅尔文取得联系？或者，是否有可能真正的杀手听说了这次脱口秀的内容，因此产生了这个想法：故意联系梅尔文，把自己和一位与毫无关系的人联系到一起混淆视听？

格雷史密斯猜测另两起谋杀案有可能是黄道十二宫杀手的第8起谋杀，但是这两位受害者中，其中一位［利昂娜·拉雷尔·罗伯茨（Leona Larell Roberts）］的情况完全不符合黄道十二宫杀手的风格，而另一位受害者伊莱恩·戴维斯（Elaine Davis）则从来没有被发现，因此根本无法把该案与黄道十二宫杀手的作案方式进行比较。我个人更相信凯莱赫和范纳伊斯的说法，也就是说斯泰恩就是黄道十二宫杀手的最后一名受害者。这封信再次强化了凯莱赫和范纳伊斯的理论，即凶手因为害怕警方的追捕而不再冲动杀人。正是因为凶手感到了恐惧，他才会想到律师。一个完全不担心被警方抓住的人是不会去寻求律师的帮助的。如果凶手真的需要别人帮助他停手，他应该联系医生、精神病专家，或者宗教人员，而不应该去联系律师。

在凶手的信件中，他反复表示害怕控制不住自己。这种恐惧是真实存在的吗？在大约3个月以后，又发生了一起案件。当我们分析这起案

件时，需要进一步考虑这个问题。

旧金山市的新案件



当晚接近午夜时，凯瑟琳·约翰斯（Kathleen Johns）正开车离开加利福尼亚州莫德斯托市。当时，她怀有7个月的身孕，并且车上还有她10个月大的女儿。当凯瑟琳快要开上132号公路（朝西的一侧）的时候，后面一辆车中的男性司机突然开始闪车灯并且按喇叭。此举引起了凯瑟琳的注意。接着，后车司机加速行驶到凯瑟琳身边，并且大声告诉凯瑟琳她的左后轮胎在摇晃。凯瑟琳虽然很害怕，但最终还是决定停车。而那名向凯瑟琳喊叫的司机则把车停在了凯瑟琳的车后。这名男司机声称自己有拆轮胎棒，可以帮助凯瑟琳拧紧固定轮胎的螺母。在“修好”了凯瑟琳的车以后，这名男子回到车中，并且开走了。

当凯瑟琳再次试图发动汽车的时候，她的左后轮马上就掉了下来。似乎这名男子不是把固定轮胎的螺母拧紧了，而是直接把螺母取了下来。此时，这名男司机的车还没有开远，于是他倒车回到了凯瑟琳停车的地方，并且对凯瑟琳说：“天哪，这个麻烦比我想象的还要严重！”也就是说，他在暗示，凯瑟琳的车并不是因为他动了手脚才出问题的。然后，这名男子提出，他可以开车送凯瑟琳去服务站。

服务站就在路前方大约1/4英里的地方。当时，凯瑟琳用肉眼就可以看到服务站，但她没有选择自己走到服务站，而是接受了这名男士的邀请，坐进了他的车里。在凯瑟琳上车以后，这名男子立刻开过了服务站，把车开上了一条废弃的农场路。途中，该男子多次把车停在路边，但又多次重新回到路上继续行驶。这位男子不断地告诉凯瑟琳，“你知

道我会杀了你的”，“你知道你就要死了”。[注]他们就这样继续在当地的小路上行驶了2~3个小时。

接着，这名男子犯了一个错误，他不小心把车开上了高速公路的出口匝道。此时，凯瑟琳意识到，她终于有机会逃脱了。当这名男子停车的时候，凯瑟琳怀抱着女儿逃到了车外。因为当时找不到人求助，凯瑟琳只好躲在一个用于灌溉的沟里。这名男司机拿出一个手电筒开始搜索凯瑟琳，然而还没等他找到凯瑟琳，一位正要通过这条匝道驶下高速的卡车司机看到了停在路边的这辆车，并且猛地拉下了手刹。这名卡车司机走下他的半拖车，并且大声喊道：“到底出了什么事？”于是，男司机立刻逃回自己的车中，并且快速开车逃走了。显然，这名歹徒并不是一个非常勇敢的猎杀者！

此时，获救的凯瑟琳由于过于恐惧实在不敢再搭任何人的车了。但是这名卡车司机一直留在现场，直到一名女性驾车经过这里。凯瑟琳坐上了这名女司机的车，后者将凯瑟琳送到了警察局。当凯瑟琳向警察讲述她的经历时，她发现警察局中的一张通缉告示上画着黄道十二宫杀手的综合素描图。凯瑟琳立刻认出，海报上的那个男人就是刚才想要杀她的人。事后，警察找到了凯瑟琳的车。有人重新装上了凯瑟琳的车的轮胎，并把车开到了另一个地点，放火烧掉了那辆车。

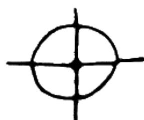
在这起案件中，有若干非常重要的问题尚未被解答。为什么这名司机在绑架凯瑟琳之后又行驶了若干个小时？为什么他不断地把车停在路边，却又不断地重新开回去？在这若干个小时的过程中，凯瑟琳每分钟都在想自己是否会死去，歹徒这么做是否只是为了享受凯瑟琳的痛苦呢？他是为了满足自己变态的快感才故意拖延时间的吗？还是说他一直在和自己的邪恶冲动做斗争，就像黄道十二宫杀手在写给梅尔文·贝利的信中所说的那样？当然，也许这名歹徒只是因为害怕被捉住，才不敢继续实施自己的谋杀计划。

在一系列的袭击案中，黄道十二宫杀手表现出了他胆小的性格特征。在斯泰恩谋杀案后，凶手选择逃走并且躲避警方的追捕。而在凯瑟

琳的案件中，卡车司机一走出卡车，凶手就立即上车逃走了。而且，这名爱玩“最危险的游戏”的捕杀者喜欢把既没有武器，也没有疑心的人作为谋杀的目标。

一个多月以后，凶手似乎终于从惊吓中恢复了一些。于是，他继续进行一项比谋杀更安全的活动——写信。

1970年4月20日的信



凶手寄给《旧金山纪事报》的信的开头部分如下：

> 我是黄道十二宫杀手。
>
> 顺便问一下，上次我寄给你们的密码，你们解开了吗？
>
> 我的名字是——
>
> AEN⊕⊗K⊗M●⊥NAM
>
> 我有一点儿想知道，你们究竟出多少钱悬赏捉拿我。我希望你们知道用炸弹在警察局杀掉那个蓝色小气鬼的人不是我。虽然我曾经说过我要用炸弹杀掉学校的儿童。然而，越界进入别人的领地毕竟是不行的。但杀掉一个警察比杀掉一个孩子要光荣多了，因为警察可以开枪回击，而小孩子不可以。到目前为止，我已经杀了10个人。如果不是我的炸弹出了问题，这个数目本来会比10要大很多。之前下的那场雨把我的炸弹都淹了。

在接下来的一页纸中，凶手写道：“新炸弹是这样装好的。”然后附

了一张占据该页大部分的炸弹图。在这张图中，凶手用文字标示出各个部件，并且解释了整个系统的工作原理。在信的末尾，黄道十二宫杀手将警方嘲弄了一通，并且写出他认为到目前为止的比分情况。

又及：我希望你们在寻找被我杀死的人的身份的过程中能够获得乐趣。

黄道十二宫杀手=10，旧金山市警察局=0

此时，黄道十二宫杀手声称自己已经杀了10个人，但是这封信同样没有提供任何杀人的证据，这一点和最早的几封信大为不同。如果黄道十二宫凶手确实在继续杀人，那他为什么会突然不再提供关于谋杀的内部信息和证据了呢？经过研究，格雷史密斯认为，第9名和第10名受害者的身份分别是凯瑟琳·约翰斯（我们在上一节中提到，她被一名歹徒绑架，并在歹徒的汽车上度过了惊心动魄的几小时，但是她并没有被害）和玛丽·安托瓦妮特·安斯蒂（Marie Antoinette Anstey，1970年3月21日，有人在湖县的一条乡村道路边发现了她的尸体）。

此外，写这封信的人还给自己塑造了一种虚假的英雄形象，他在信中写道："但杀掉一个警察比杀掉一个孩子要光荣多了，因为警察可以开枪回击，而小孩子不可以。"然而，黄道十二宫杀手从未试图去杀警察。他每次都从谋杀现场逃之夭夭，以躲避警察的追捕。在斯泰恩谋杀案发生之后，黄道十二宫杀手一直躲藏在警方的视线之外。在黄道十二宫杀手所犯下的所有罪行中，根本找不到他所说的这种"光荣"，他选择攻击的对象一直是一些既没有自卫能力，又没有对凶手起疑心的人。

虽然有些人认为"我的名字是——"这条密码也是一个未解之谜，但是有人提出了这个密码的一种解法，并且我个人认为这就是正确的解法。(注)读者也许还记得，在之前的信件中，凶手曾承诺，只要解开密码，就能发现他的身份。然而，解密后的信息中根本没有发现凶手的身份信息（除非那段密码的最后几个字母并不仅仅是用来填满长方形，而

是有意义的）。在我看来，这次凶手又在拿读者开玩笑。我认为正确的密码解法是：

A L F R E D E N E U M A N（阿尔弗雷德·E.纽曼）

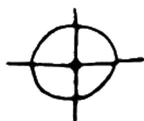
A E N ⊕ ⊗ K ⊘ M ● ⅃ N A M

这种解法并不非常完美——第3位上的N被译为字母F，但是第11位上的N却被译为字母M。但是，这种解法看起来已经非常接近完美了，并且我们知道黄道十二宫杀手在写信的时候确实常常会出现各种错误。

对于那些不太了解流行文化的读者，我想我有必要解释一下，阿尔弗雷德·E.纽曼是幽默期刊《疯狂杂志》（*Mad Magazine*）上的一个类似吉祥物的卡通形象，从20世纪50年代中期就已经有了。

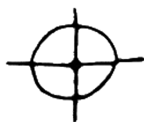
8天以后，凶手似乎仍然担心会被警方抓住。因此，当他再次出击的时候，他仍然没有杀人，而是寄出了另一张贺卡。

1970年4月28日的信



《旧金山纪事报》收到的这张贺卡内的信息如下：

I hope you enjoy your selves when I have my Blast.



当我引发爆炸时，我希望你们能感到愉快。

此外，这张贺卡的背面还有一段“后记”，比贺卡中的信息还要长，其内容如下：

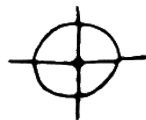
如果你们不想让我实施爆炸，你们必须做两件事情。第一，向所有人公布公共汽车炸弹的所有细节。第二，我希望能在城镇的各个地方看到好看的黄道十二宫标志。其他人都有各种标志，比如世界和平标志☮、黑暗力量标志、梅尔文吃鲸油标志等。如果我看到许多人佩戴了我的黄道十二宫标志，我会非常高兴的。请不要佩戴那些讨厌的标志，比如梅尔文的标志。

谢谢你

格雷史密斯写道：“当然，此后并没有人佩戴黄道十二宫的标志。”[注]某些朋克摇滚人确实制造了一些黄道十二宫的标志，但是他们佩戴这些标志的目的是为了反讽。

在接下来的大约两个月的时间中，公众都没有再次听到黄道十二宫凶手的消息。

1970年6月26日的信



接着，黄道十二宫凶手在当年6月底又向《旧金山纪事报》发去了

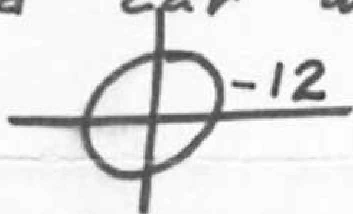
一封信。由于这封信的内容特别有趣，我把这封信的完整图像复制在图4–7中，而不是像之前那样仅抄录信中的文字。

凶手在这封信中描述的谋杀案确有其事，但警方已经对一名不是黄道十二宫杀手的嫌疑人签发了逮捕令。此外，凶手未能在信中提供任何公众不知道的凶案细节。因此，我们有相当充分的理由相信，黄道十二宫杀手事实上与这封信中提到的这起凶案案并无关系。

这封信中的密码至今还没有任何人能够解开。但是这封信有一个与之前的所有信件都不一样的特点，那就是信中附有一张地图。我把这张地图复制在图4–8中。

This is the Zodiac speaking

I have become very upset with the people of San Fran Bay Area. They have <u>not</u> complied with my wishes for them to wear some nice ⊕ buttons. I promiced to punish them if they did not comply, by anilating a full School Buss. But now school is out for the summer, so I punished them in an another way. I shot a man sitting in a parked car with a .38.



SFPD-0

The Map coupled with this code will tell you where the bomb is set. You have untill next Fall to dig it up. ⊕

C △ J I ■ O ꓘ ⫫ A M ⅂ ▲ Ω O R T G
X ⊙ F D V ꞇ ◪ H C E L ⊕ P W △

图4-7 1970年6月26日的信件（随信附有一段密码和一张地图）

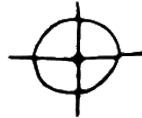
当时，没有任何人知道凶手寄来的这段密码和地图之间究竟有什么联系。在这张地图上画有一个符号，很像是凶手的签名。这个符号的中心点在迪亚布洛山，更具体来说，符号的中心点落在迪亚布洛山南峰的一个海军无线电站处，虽然在凶手寄来的这张地图上并没有明确标出这里有一个海军无线电站。

图中的文字可译为：

我是黄道十二宫杀手。

我对旧金山湾区的人们非常失望。因为他们没有服从我的意愿佩戴好看的黄道十二宫标志。我说过，如果他们不服从的话，我就要炸掉一辆满员的校车来惩罚他们。但是现在学校已经放暑假了，因此我决定用另一种方式惩罚他们。我用一把0.38英寸口径的手枪打死了一个坐在车中的人。

黄道十二宫杀手—12，旧金山警察局—0

这段密码和信中所附地图能够告诉你们我将炸弹放置在何处。你们需要在明年秋天之前解开这段密码。

凶手在这封信中所附的密码至今尚未被解开，但是对于这个密码的破解，我有一个值得考虑的想法。也许，凶手为了不让自己的密码被破译，对密码中的字母替换法则进行了很大的改动。在已被破译的3段密码中，没有任何一个字母是由本身表示的。所以，在这段新密码中，我认为凶手有可能会让若干个字母代表它们本身，因为凶手认为试图破译这段密码的人不会想到这种可能性。我认为，第一个词可能是“CALIFORNIA（加利福尼亚州）”，在这种解法中，字母C、I、O、A分别代表本身。明文在O和A之间缺了一个字母，但是既然

凶手经常拼错单词，这样的情况也是合理的。在本章之后的内容中，我会利用凶手此后寄来的另一封信中的一条线索，进一步讨论我对目前这封信中的密码余下部分的猜测。然而，在提到那封信之前，我们先来看凶手接下来的一封信，这封信中既没有密码，也没有提供任何线索。

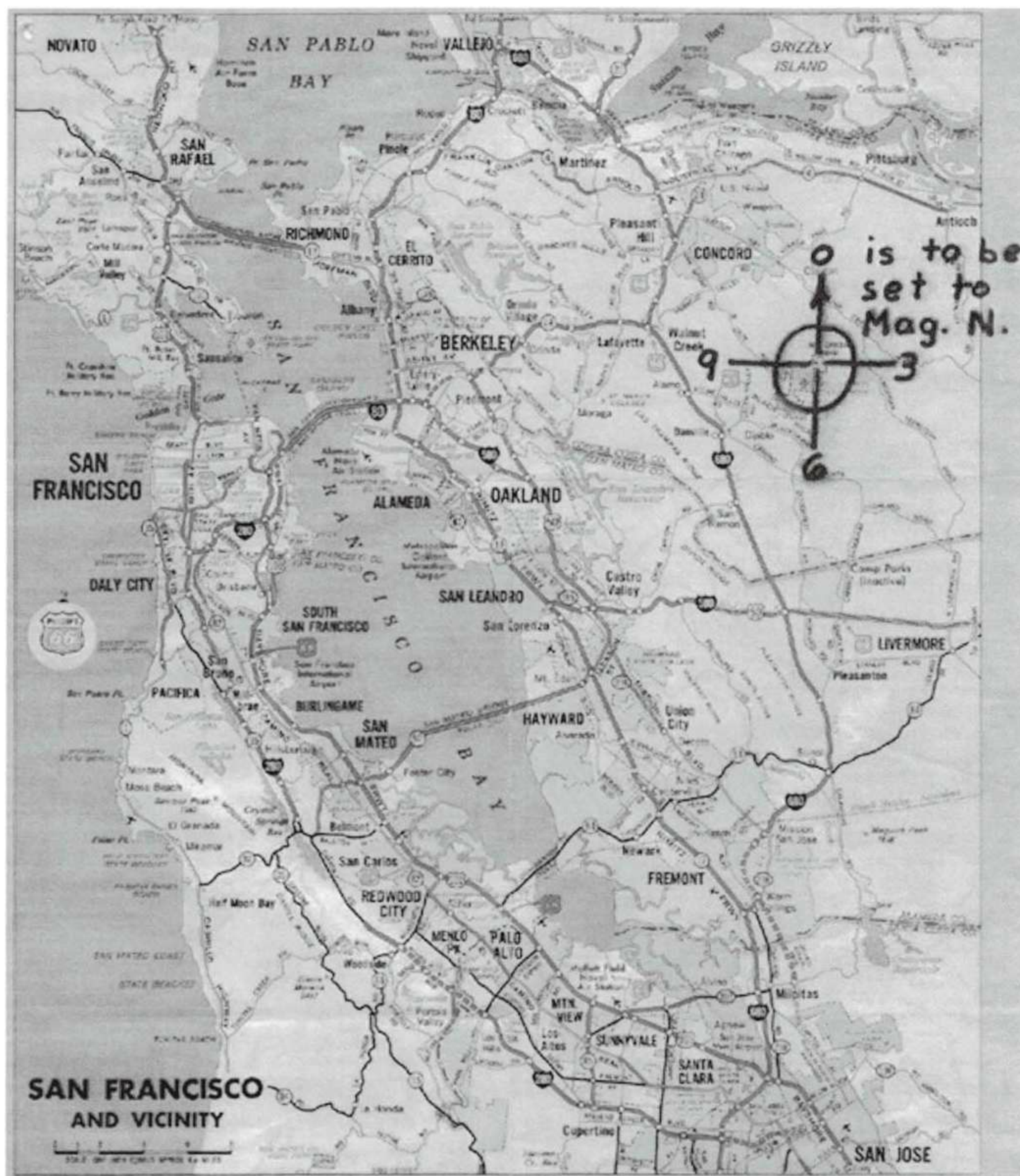
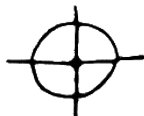


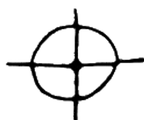
图4-8 这张地图是否有可能为我们提供解开密码和凶杀案的钥匙？

1970年7月24日的信



在当年的7月份走向尾声时，黄道十二宫杀手再次给《旧金山纪事报》写信，似乎他觉得有必要再次讨论黄道十二宫标志的问题。

> 我是黄道十二宫杀手。
>
> 你们这些人不肯佩戴好看的黄道十二宫标志，这让我相当不悦。因此，现在我要向你们提供一份小小的名单。这份名单的开头是那个女人+她的婴儿，几个月之前的某个夜晚，我载她们经历了一段长达数小时的有趣的汽车之旅。最后，我在发现她们的地点烧掉了这个女人的汽车。

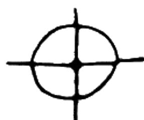


这封信的内容似乎确认了凯瑟琳·约翰斯遇到的那名歹徒就是黄道十二宫杀手。如果情况确实是这样，我们就面临一个非常有趣的心理学问题。在凯瑟琳·约翰斯绑架案中，凶手并没有像之前那样杀掉被害者。因此，我们要再次提出那个问题：凶手是在有意识地控制自己吗？还是害怕被警察抓住的恐惧已经令凶手无法完整地实施谋杀计划了？也许，凶手只是缺乏再次下手的胆量而已。

两天之后，《旧金山纪事报》又收到了凶手的另一封信。下面这封

信也许是黄道十二宫杀手的所有信件中为警方的破案工作提供线索最多的一封。

1970年7月26日的信



7月26日的这封信大部分都是在抄写吉尔伯特（W.S.Gilbert）和沙利文（A.Sullivan）的歌剧《天皇》（*The Mikado*）中《一个更富人性的天皇》（A More Humane Mikado）和《某一天它可能会发生》（As Some Day It May Happen）两个曲目的唱词。当然，信中有许多错误，凶手也许是故意抄错的，也许是无意的。但是，这封信还有一段非常有趣的后记，这段后记与凶手的上一段密码有关。因此，请读者耐心地读完这封信，最重要的内容在信的末尾！

我是黄道十二宫杀手。

既然你们不愿意佩戴好看的黄道十二宫标志，那么要不要佩戴一些难看的黄道十二宫标志呢？或者任何你们能够想到的黄道十二宫标志都可以。如果你们不肯佩戴任何形式的黄道十二宫标志，那么（在所有其他的事情之外）我就会折磨在天堂中等着我的13个奴隶。我会把其中一些奴隶绑在蚂蚁山上，看他们尖叫+抽搐和扭动。我会把松木的碎片插入另一些奴隶的指甲下面+然后烧掉。另一些奴隶会被我关在笼子里，我会给他们喂咸牛肉直到再也塞不下去，然后我会倾听他们哀求我，让我给他们水，而我只会嘲笑他们。还有一些奴隶，我会系住他们的拇指把他们吊起来+在太阳下炙烤，然后我会给他们抹热力镇痛膏来给他们暖身。还有一些奴隶，我会活剥了他们的皮+让他们尖叫着跑来跑去。所有打台球的人，我会让他们

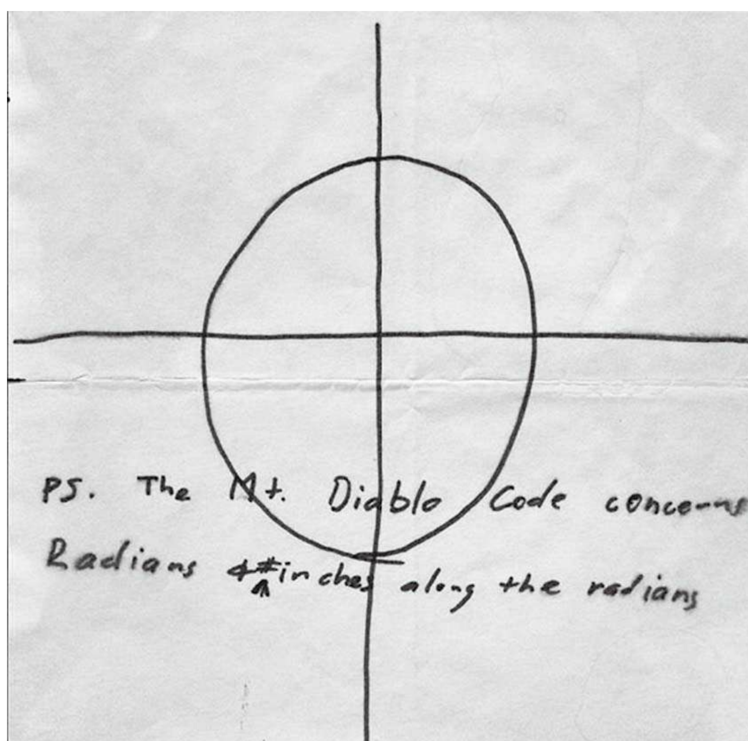
在黑暗的地牢里用弯曲的球杆+穿着扭曲的鞋子打台球。在给我的奴隶们带来最可口的痛苦的过程中，我会得到许多乐趣。

旧金山警察局=0 ⊕ =13

某一天，一名受害者终将被找到。我有一份小小的清单。我有一份小小的清单，清单上是一些社会的罪人，他们即使到了地下，也不会有人想念他们，也不会有人想念他们。讨厌他们的人们会在上面签上名，还有所有有着松弛手臂和令人讨厌的笑声的人们。所有用im- platt请求你的约会中的孩子们。所有握手的人，像那样握着手。所有未被损坏的第三人带走所有坚持的人。他们都不会被想念。他们都不会被想念。其中有一位班卓琴小夜曲演奏者，还有他的同族，还有一位钢琴管风琴演奏者，我把他也加入我的清单。所有吃薄荷糖和你脸上的phomphit的人，他们都不会被想念。他们都不会被想念。那些傻瓜，只会用热情的语调赞美其他世纪，却不赞美这个世纪，只会赞美其他国家，却不赞美他们自己的国家。还有来自外省的女人，穿得像个不会哭的男人。还有奇怪的异常的女孩，她从来没亲吻过。我不信任何人会想念她，我确定没有任何人会想念她。还有那个友善的impriest，相当普遍，那个法庭上的幽默者，我把他加入我的清单。所有滑稽的人，喜剧演员，私人生活中的小丑。他们之中哪个都不会被想念。他们之中哪个都不会被想念。还有那些没前途的人，比如那个谁谁谁，那个啥啥啥等。好吧，别在意，啧啧啧啧，还有那些不知道名字的人，还有你认识的人，但是我把填空的工作留给你。但是你把谁放在清单上真的无所谓，因为他们都不会被想念。他们都不会被想念。

又及：迪亚布洛山的密码与弧度，以及弧度上的英寸数有关。

这段后记值得放大仔细研究。我把原信的这部分图案复制于图4–9中。



PS. The Mt. Diablo Code concerns
Radians & # inches along the radians

图4-9 关于最近一段密码的一条线索

所以，从这封信中我们可以确认两件事情：第一，这个杀手大概没法以写作谋生；第二，这名杀手知道“弧度”这个概念。对于不熟悉这个概念的读者，我有必要介绍一下：弧度是一个用来度量角度的概念。对于大部分人来说，我们在学校里最先学到的度量角度的单位是度数。一个完整的圆的角度是360度，但是360这个数字是人工创造的。我们之所以用360表示一个整圆的度数，可能是因为一年中大约有360天，或者也可能是因为古代的苏美尔人使用一种60进制的计数系统（但是苏美尔人选择60进制的计数系统可能也是受到了一年中包含的天数的影响）。不管怎么说，事实上并没有任何理由一定要把一个圆分成360份，每份对应于1度。我们也可以用其他数目来定义一个完整的圆的度数。

而与角度不同的是，弧度的度量却是自然的。让我们来看一看图4–10中画的这个角。

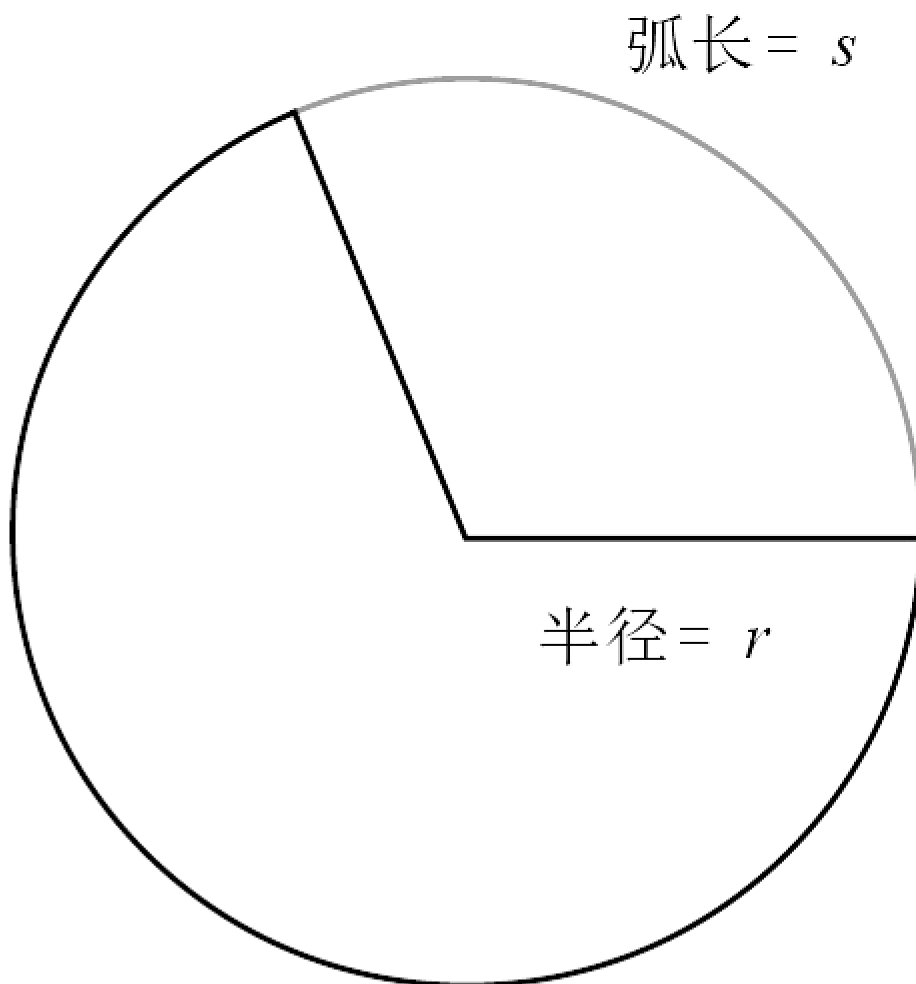


图4-10 用弧度来度量角

我们将弧度定义为s/r，其中s表示圆周上的弧长，r表示圆的半径。用弧度来度量角度的优势在于，它并没有把一个整圆的度数人为地设定为某个数值，而是利用以上的公式自动给出一个数值。一个圆的周长是$2\pi r$，因此它的总角度是$2\pi r/r = 2\pi \approx 6.28$。

如果我们希望一段圆弧的弧度正好等于1，那么就必须让这段弧长和圆的半径相等。此时，圆弧的角度大约是57.296度。

那么，为什么一位连环杀手要谈论“弧度”这个数学概念呢？黄道十二宫杀手是否拥有比普通人更深厚的数学背景？

加雷思·佩恩提出了一种理论，能把黄道十二宫杀手的第四段密码

所附的地图与弧度联系起来。用他自己的话来说，他的理论是这样的：

> 我发现，如果把迪亚布洛山的顶峰当作一个扇形的顶点，然后让扇形的一条半径通过蓝岩泉谋杀案发生的地点，另一条半径通过旧金山市的普雷西迪奥高地（也就是黄道十二宫杀手杀死出租车司机保罗·斯泰恩的地点），那么这个扇形的弧度正好是1。突然之间，我看出这是一个和数学有关的设计。这个发现让我震惊、恐惧，到了几乎要呕吐的程度。黄道十二宫杀手一直在根据旧金山湾区的地图进行一种巨大的几何设计，那些受害者的生命对他来说只是这个设计中的标示点而已。(注)

图4–11用地图解释了上述理论。

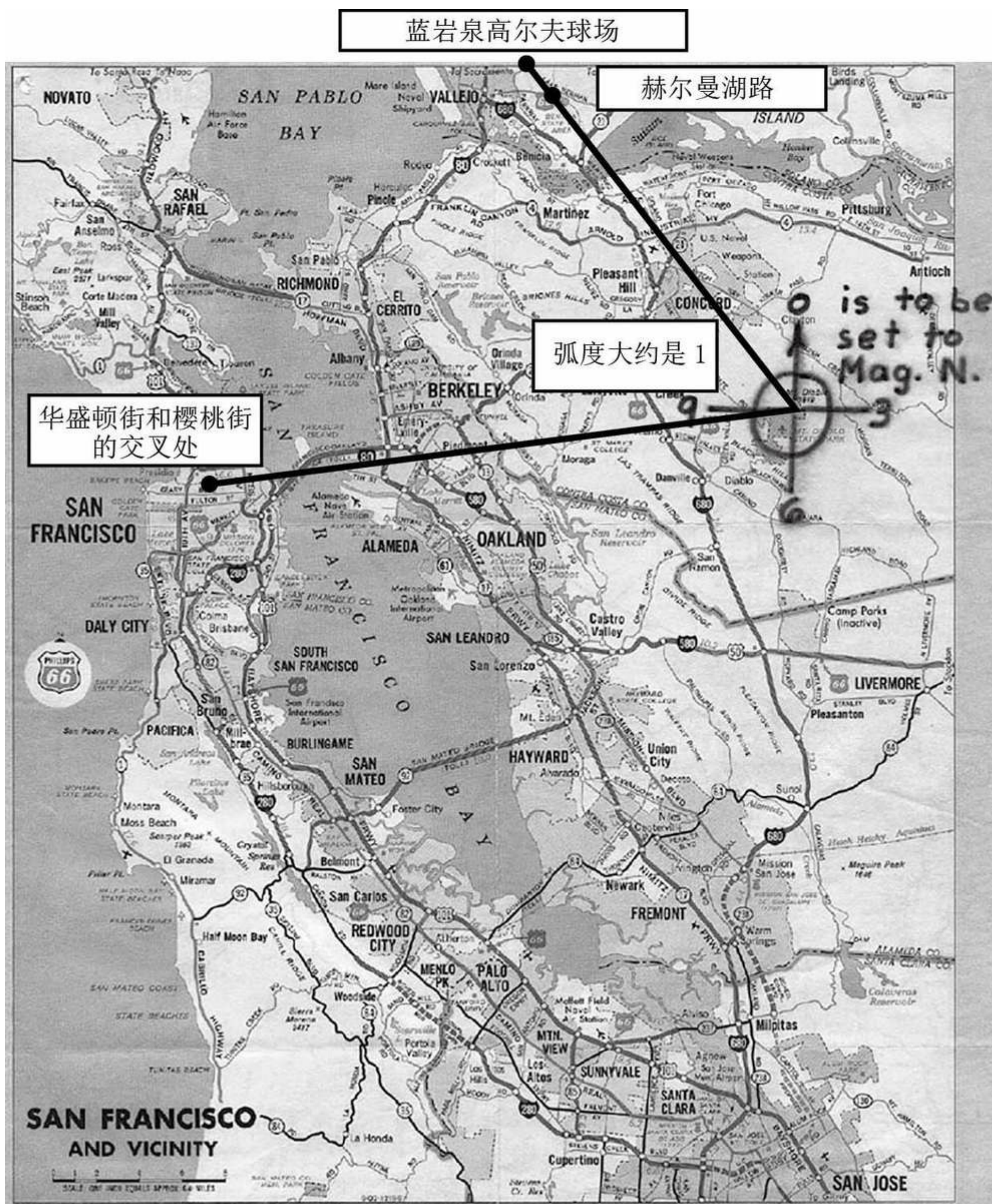


图4-11 解释弧度理论的一张地图，上面做了标记

有了上述发现以后，佩恩对凶手及侦查该案的警方的智力水平进行

了重新评估。他写道：

> 当我发现那么多无辜的生命死于这样一个无聊的目的，当我发现在凶手愚蠢的面具下隐藏的竟然是这样一个冷酷无情、精于算计、智力极高的灵魂，我受到了深深的震惊。让我同样震惊的是，收到这封信已经10多年了，警方却从未对弧度理论进行过研究。事实上，在面对这个谜题的10多年时间中，警方甚至从未劳神翻开字典查查“弧度”这个词是什么意思。多年以来，警方一直不理解黄道十二宫杀手为什么要谋杀旧金山市的那位出租车司机，当我告诉警方“弧度”这条信息的重要性时，他们立刻理解了出租车司机被杀的原因。接下来，警方又花了大概两个星期的时间，才把我提供的这条信息提升至“重点怀疑”状态。然后，当警方发现我所使用的工具仅包括一部字典和一个量角器以后，他们立刻失去了兴趣，并将他们的注意力转向了其他“更加急迫的事情”。(注)

接着，佩恩又进一步“赞扬”了执法部门的能力，他写道：“我的另外一些研究显示，湾区警方十分博学地认为π = 3.1，并且认为大于12的二进制数无法被写下来。”(注)

佩恩的这些研究提醒了我们一个非常有趣的事实，那就是：只有少数的职业会用到“以弧度度量角度”的数学知识。即使有些人在高中数学课或者大学数学课上学过这条知识，如果他们在工作中没有用到它的话，这条知识恐怕也不会长期被存储在记忆中。因此，我们不禁要问这样一个问题：为什么黄道十二宫杀手不仅知道弧度的含义，并且还在给警方的信件中使用这一概念呢？黄道十二宫杀手是否从事某种能用到弧度概念的职业呢？事实上，除了用到弧度以外，有多条证据都显示，虽然黄道十二宫杀手的信件中充满了拼写错误，实际上他却比他看起来聪明得多。如果情况确实是这样，那么黄道十二宫杀手在这些信件中的大量拼写错误很可能是有意为之的。在这些信件中，写信人虽然把许多简单的单词拼错了，但有时一些复杂单词的拼写反而是完全正确的。

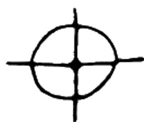
根据弧度理论，黄道十二宫杀手谋杀斯泰恩可能有两重动机。第一，出租车司机可以带凶手去任何他想要去的地方。既然凶手希望两件谋杀案分别发生在以迪亚布洛山为顶点的扇形的两条半径上，他就必须在特定的地点实施谋杀。为了达到这个目的，出租车司机是比较方便的谋杀对象。第二，在黄道十二宫杀手此前的几次谋杀中，凶手意外地让男性受害者活了下来。因此，在心理上，凶手可能认为有必要证明自己不仅可以杀死女人，也同样可以杀死男人。于是斯泰恩的性别也符合凶手的需要。

有些研究者指出，这两起谋杀案所形成的角度并不正好是1弧度，而是比1稍大一些，在60度左右（即1.047弧度）。[注]但是，对于像黄道十二宫杀手这样疯狂的人来说，我们真的有必要纠结0.047的误差吗？我个人认为，佩恩提出的弧度理论正是黄道十二宫杀手的原意。但是，对于佩恩所著书籍中的许多其他内容（比如黄道十二宫杀手的身份），我则持强烈反对的态度。我认为，佩恩对凶手身份的论断事实上产生了一个新的受害者：一个无辜的人被佩恩公然指认为这些残忍凶案的凶手，这是很不公平的。

除了佩恩指认的这个人以外，在各种各样的网络资源、书籍，以及电子书中，还有许多其他人被指为黄道十二宫杀手。虽然黄道十二宫杀手有可能曾因为其他罪行在监狱中待过，但是我们可以肯定的是，警方从来没有以本章描述的这些凶案为理由对任何人提起诉讼。因此，关于黄道十二宫杀手的身份，存在大量怀疑和猜测的空间。目前，已经有几个人声称他们的父亲就是黄道十二宫杀手本人，此外，还有一些人声称他们的前夫是黄道十二宫杀手。在没有确切证据的情况下，我不希望随意指认某些人为凶手。因为在所有这些嫌疑人中，不太可能有多人同时都是黄道十二宫凶手，所以，除了凶手本人以外，所有的嫌疑人其实都是流言的受害者。如果读者有兴趣的话，要找出一些有犯案嫌疑的人并不困难。事实上，在本章的参考书目中，我也列出了一些包含这方面讨论的文献。但是，在本书中，我不打算指认任何人为黄道十二宫杀手。

那么，这条关于弧度的线索对我们而言还有用吗？凶手的提示中包含“英寸数”的字样，因此，我认为这封信中接下来的一段密码中［即我认为以“CALIFORNIA（加利福尼亚州）”开头的那段密码］应该包含数字。此外，这段密码中还可能包含“INCH（英寸）”一词或者“INCHES（英寸的复数形式）”一词。而如果数字中有小数点的话，“POINT（点）”一词也有可能出现。在前文中，我们曾经介绍过密码分析技巧中的“可能词搜索”，以上我所列出的这些词都是值得尝试的“可能词”。当然，还存在许多其他可能性。即使这段密码的第一个词确实是“CALIFORNIA”，这条信息所能提供的帮助也不大，因为在这个单词中只有3个字母再次出现在密码的其他部分中。也许，“CALIFORNIA”一词给我们提供的最重要的线索是，这段密码的最后一个字母是用一个三角形符号代表的字母A（这个符号看起来确实有些像字母A）。以字母A结尾的英语单词并不多。根据某项统计研究，在有意义的英文单词中，每1 000个英语单词中只有24.7个单词是以字母A结尾的。[注]也就是说，只有2.47%的单词以字母A结尾。并且，这还包含单个字母A作为单词的情况。由于这条信息不太可能以单字母单词“A”结尾[注]，所以，最后一个单词是A的可能性实际上远远低于2.47%。不管怎么说，我写下了这条意见，也许某位读者可以根据这条意见得出某个有用的结论。但也有可能我指出的是一个完全错误的方向！请读者自行判断吧。

故事尚未结束

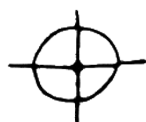


此后，还出现过其他来自黄道十二宫杀手的信件，一般认为这些信

件确实出自凶手本人。但是，在这些信件中凶手再也没有给出任何新密码，因此我将不再赘述这些信件的内容。值得注意的是，其中两封信件之间的时间间隔较长，表明凶手可能在此期间因为某些较轻的罪行进过监狱。凶手曾在1971年3月22日写过一封信，而下一封信则写于1974年1月29日，在这两个日期之间没有任何其他信件。根据凶手自己在信中的说法，受害者的数目已经增长到37个。但我认为，这个数字完全是凶手虚构出来的。㊟在所有这些信件中，没有任何证据显示黄道十二宫凶手在斯泰恩以后还谋杀过任何人。在前文中我们已经详细地描述过，在斯泰恩谋杀案发生之后，黄道十二宫凶手差点儿被警察当场抓住。因此，凶手此后可能已经没有勇气制造新的罪案，他只是一直在通过信件虚张声势而已。虽然，黄道十二宫杀手在信中提到的有些受害者确实死于谋杀，但是他没有能够提供任何证据，证明自己是这些谋杀案的凶手。关于这些谋杀案，他所了解的一切信息都仅限于报纸报道的那部分。在此前的信件中，黄道十二宫杀手非常喜欢提供关于罪案的内部信息，甚至物理证据。因此，如果后期的这些罪案确实也是他犯下的话，他没有理由不继续提供这些内部信息和物理证据。

当然，关于这一点，也有许多研究者与我的看法截然不同。如果读者想了解这些与我不同的看法，可以参考罗伯特·格雷史密斯的优秀著作《十二宫》（*Zodiac*）。在这本书中，格雷史密斯列出了一份名单，包含49名“被黄道十二宫杀手所杀，或者可能被黄道十二宫杀手所杀的受害者”。㊟

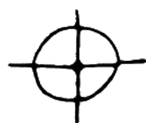
谁是第一个受害者？



某些研究者认为，黄道十二宫凶手在斯泰恩以后还谋杀过其他受害者。也有一些研究者认为，本章开头提到的贝蒂·卢·詹森和戴维·阿瑟·法拉第谋杀案并不是黄道十二宫杀手犯下的第一件谋杀案。有的研究者怀疑，黄道十二宫杀手的第一个受害者是里弗赛德社区大学的大一新生切里·乔·贝茨（Cheri Jo Bates）。切里·乔·贝茨于1966年10月30日在大学图书馆旁边的一处停车场中受到攻击。她死于多处刀伤，其中一刀切断了颈动脉。虽然贝茨一案的某些细节确实与黄道十二宫杀手所犯下的其他罪案有一些相似之处，比如此案的凶手也在作案后向里弗赛德《企业报》（*Press-Enterprise*）发去了一封信等，但我认为贝茨谋杀案并不是黄道十二宫杀手所为。[注] 1971年3月13日，黄道十二宫杀手确实给《洛杉矶时报》（*Los Angeles Times*）写信，声称自己是杀害贝茨的凶手，然而此时距那篇首次将贝茨案与黄道十二宫杀手联系起来的新闻报道已经有4个月的时间了。并且，在黄道十二宫杀手写给《洛杉矶时报》的这封信中，没有提供任何证明贝茨一案与黄道十二宫杀手有关的证据。

但是在格雷史密斯的《十二宫》中，作者认为贝茨“绝对是受黄道十二宫杀手所害”。[注]

流行文化的关注



黄道十二宫杀手和开膛手杰克一样引起了流行文化的巨大关注，这其中最大的原因恐怕就是黄道十二宫杀手和开膛手杰克一样逃过了法律的制裁。以黄道十二宫杀手所犯下的罪案为题材的第一部电影是《黄道十二宫杀手》（*The Zodiac Killer*），该片于1971年4月上映。同年12月，另外一部电影——由克林特·伊斯特伍德（Clint Eastwood）主演的

《肮脏的哈里》（*Dirty Harry*）也上映了。《肮脏的哈里》大致以黄道十二宫系列谋杀案为基础，并且把地点也设置于斯泰恩谋杀案发生的旧金山市，还让凶手自称“天蝎宫杀手”（Scorpio），对应“黄道十二宫杀手”（Zodiac）。不过，现实中的黄道十二宫杀手只是威胁要用炸弹袭击学校的校车，而在这部电影中，凶手真的袭击了一辆满载学生的校车——当然，这也是好莱坞电影的典型夸张手法。这部电影与现实的另一处区别是，最后凶手被绳之以法，我想，这也许是现实世界中的群众最想看到的黄道十二宫连环凶杀案的结局吧。2005年上映了乌利·隆梅尔（Ulli Lommel）导演的成本极低的小制作电影《十二宫杀手》（*Zodiac Killer*）[注]，同年还上映了另一部题为《黄道十二宫》（*The Zodiac*）[注]的电影。此后，2007年又上映了一部更加优秀的黄道十二宫杀手电影[注]，这部电影名为《十二宫》（*Zodiac*），是根据罗伯特·格雷史密斯的同名著作改编的。

因1971年的小说《驱魔人》（*Exorcist*）以及据其改编的著名电影而闻名于世的小说家威廉·皮特·布拉蒂（William Peter Blatty）还写过一本《驱魔人》的续集，这本书叫作《群魔》（*Legion*）。《群魔》一书中的凶手同样也是以黄道十二宫杀手为原型，凶手自称“双子宫杀手”（Gemini Killer）。除此之外，还有许多其他受到黄道十二宫杀手启发而写成的小说，虽然它们也得到出版发行，但是这些小说实际上只能说是黄道十二宫杀手的“同人文”。在这里我不打算向读者介绍这些小说的具体内容。我也同样不打算向读者介绍各种声称“我的亲戚是黄道十二宫杀手”的书籍，但是我在书尾的“参考文献及延伸阅读”部分中列出了几本这类书籍，有兴趣的读者可以自行阅读。

和伏尼契手稿一样，未破解的黄道十二宫杀手密码（尤其是340密码）也引起了许多密码破译者的兴趣，因此所谓的“破译结果”也有不少。我之所以提到了格雷史密斯的解法，是因为他对黄道十二宫连环凶杀案有非常深入的了解，而在我看来，其他的“破译结果”都是没有价值的。

然而，关于密码的技术和科学都在不断地进步，计算机的计算能力也正在变得越来越强大。虽然我并不期望这些未被解开的黄道十二宫密码能够直接告诉我们凶手的身份，但是如果有一天这些密码真的被破解，也许我们能够获取一些新的线索，而这些新线索或许能帮助我们解开案件的真相。

---

1. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 30.
2. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 32–33.
3. “免下车”（drive-in）餐馆是美国的一种餐馆形式，顾客可以开车从窗口点餐取餐，全程不需要下车。——译者注
4. Images from Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 50–51.
5. cribbing一词是指在不认识某段文字的情况下把它照抄一遍。——译者注
6. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 58 for some “solutions.”
7. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 67.
8. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 69.
9. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 71.
10. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 75.
11. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 83.
12. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 85 and 91.
13. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 91.
14. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 102.
15. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 107.
16. Michael D.Kelleher and David van Nuys, “This Is the Zodiac Speaking”: Into the Mind of a Serial Killer (Westport, CT: Praeger, 2001).
17. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 122.
18. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 243.
19. 赫布·凯恩是《旧金山纪事报》的一名记者。——译者注
20. 此处的“Christmass”词尾多了一个“s”，是凶手的拼写错误。——编者注
21. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 136–37.

22. Robert Graysmith, Zodiac Unmasked: The Identity of America’s Most Elusive Serial Killer Revealed (New York: Berkley Books, 2002), 128.

23. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 148.

24. Gareth Penn, “The Calculus of Evil,” MENSA Bulletin, no. 288 (July/August 1985): 5–8, 25, p. 5 quoted here.

25. Gareth Penn, “The Calculus of Evil,” MENSA Bulletin, no. 288 (July/August 1985), 5–8, 25, p. 5 quoted here.

26. Gareth Penn, “The Calculus of Evil,” MENSA Bulletin, no. 288 (July/August 1985), 5–8, 25, p. 25 quoted here. Also see Gareth Penn, Times 17: The Amazing Story of the Zodiac Murders in Cali-fornia and Massachusetts 1966–1981 (New York: Foxglove Press, 1987), 26.

27. http://www.zodiackillerfacts.com/Ray%20Grant.htm.

28. Fletcher Pratt, Secret and Urgent (New York: Bobbs-Merrill, 1939), 258. This is a book used by Harden!

29. “A”作为单字母的单词意为“一个”，一般不会出现在句子末尾。——译者注

30. See the killer’s letter of January 29, 1974, for the claim of thirty-seven victims. Available online at http://www.zodiackillerfacts.com/gallery/thumbnails.php?album=19.

31. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 308–11.

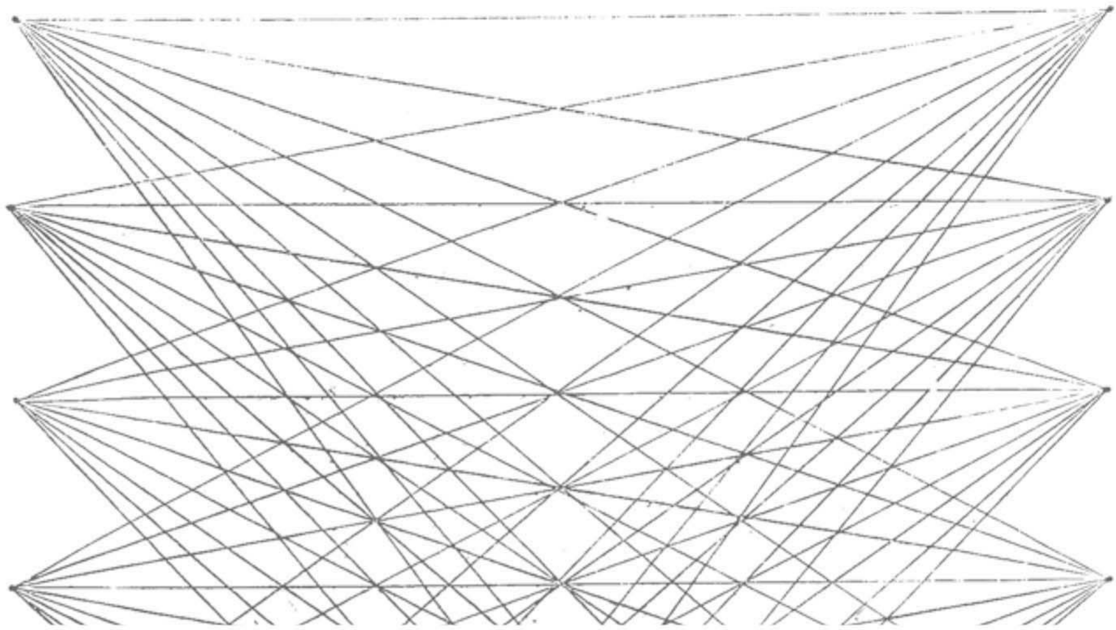
32. I refer the interested reader to Kelleher and Van Nuys, “This Is the Zodiac Speaking” again. Their argument against Zodiac being connected with Bates is persuasive.

33. Robert Graysmith, Zodiac (New York: St. Martin’s/Marek, 1986), 308.

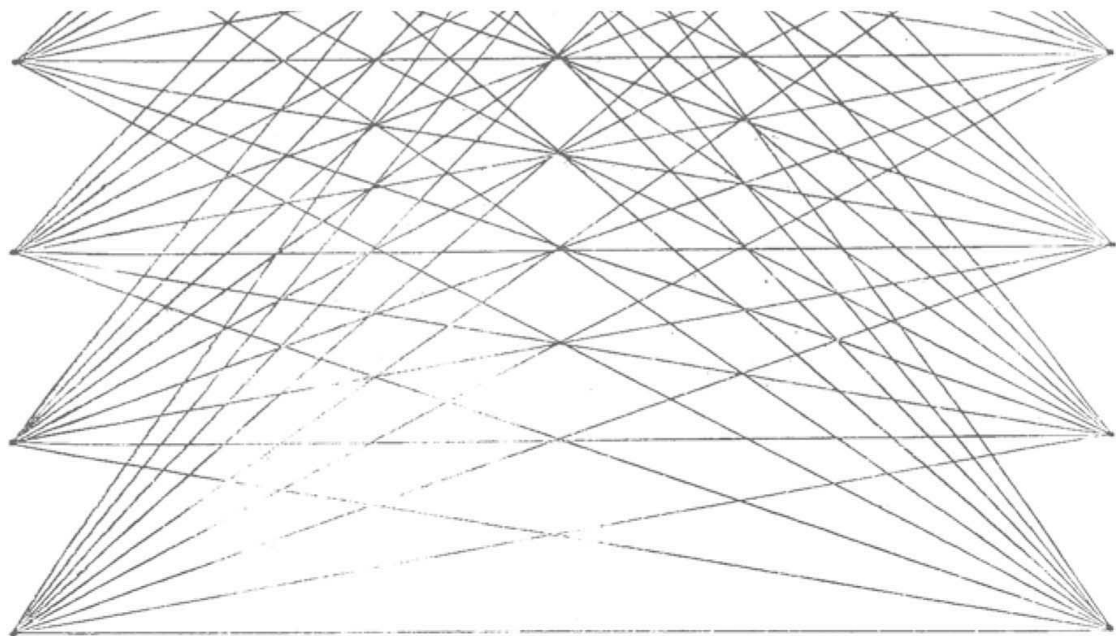
34. http://www.imdb.com/title/tt0469999/.

35. http://www.imdb.com/title/tt0371739/.

36. http://www.imdb.com/title/tt0443706/.

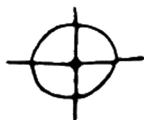


第5章
罪案密码



与蝙蝠侠故事里的恶棍一样，现实世界中也有一些凶手故意以嘲讽或炫耀的文字留下一些关于他们所犯罪案的线索。其中有一些密码至今仍是未解之谜，比如上一章提到的黄道十二宫杀手密码就是一例。本章将继续介绍一些目前尚未解开的杀手密码。下面我们先来看一个1882—1883年发生的案件。

贝齐案



1882年5月1日，一个自称“亨利·德勒特纳克·德博斯尼斯”（Henry Deletnack Debosnys）的男人来到美国纽约州的埃塞克斯。他不仅能说6种语言，还是一位出色的画家，并且相当有魅力。也许，这些特点正是伊丽莎白·韦尔斯（昵称贝齐）被他吸引的部分原因。亨利告诉贝齐，他是从巴黎来的。贝齐自己也是一名移民，她于1840年在爱尔兰出生，在母亲去世后随父亲搬来美国居住。此后，贝齐又经历了另一起悲剧——她的第一任丈夫于1870年死于一次煤矿事故，当时贝齐正怀着他们的第4个孩子。

第一任丈夫死后，贝齐似乎并不急于再婚，她独居了12年。但在1882年6月8日，她嫁给了亨利·德博斯尼斯，此时她只认识了亨利5个星期。贝齐有多了解亨利？看起来亨利显然向贝齐隐瞒了他此前的经历：亨利结过两次婚，两任妻子都死了。在亨利搬来埃塞克斯前不到两个月，他的第二任妻子塞莱斯廷（Celestine）死于一起谋杀，犯罪嫌疑人之一正是亨利本人。

贝齐再婚并不是为了寻求经济支持，她自己的财务状况良好。事实上，在贝齐的第一任丈夫死后，她获得了一笔赔偿金。此外，贝齐还在

一个秘密的地方（她前夫在窗台下面制作了一个暗格）藏了大约300美元的现金，这样既能保证钱财的安全，又能在需要钱的时候方便地取用。除了这些现金以外，贝齐还拥有15英亩的不动产。

自从贝齐和亨利结婚以后，亨利就不断地央求贝齐把不动产的所有权转到他的名下。贝齐拒绝了亨利的这一要求，也拒绝告诉亨利她前夫的赔偿金藏在什么地方。夫妇两人经常为了这几件事争执不休，他们之间远谈不上是“恩爱夫妻”。

1882年8月1日，贝齐被发现死亡，此时距离她与亨利结婚只有不到两个月的时间。贝齐的死绝对不是事故或自然死亡，她头部中了两枪，喉咙被切开，刀口很深，一直到脊柱。由于本章要介绍好几起凶杀案中的密码，所以篇幅所限，我没有办法像上一章描写黄道十二宫连环凶杀案那样详细地列举案件的细节。如果读者有兴趣详细了解本案，可以阅读法恩斯沃思（Farnsworth）[注]所写的相关书籍。我想，以下的事实已经足够让读者对本案的性质有一个大致的了解了：法庭对亨利进行了两天的庭审，其间控方展示了大量不利于亨利的有力证据。庭审结束后，陪审团只用了9分钟就达成了对亨利的统一判决：一级谋杀罪成立。

对于亨利来说，等待庭审的过程是漫长的。虽然亨利在1882年8月就被逮捕，但是直到1883年3月6日，针对他的庭审才正式展开。在等待庭审的过程中，亨利在监狱里花了大量时间进行写作，他的作品中有很大一部分是风格阴郁的诗歌和散文。然而，这些作品中还包含了一些密码，并且至今也没有人能成功破译他的任何一段密码。我们没有办法确认亨利写下的这些密码究竟是不是英语，因为亨利的其他作品既有用英语写成的，也有用法语、希腊语、拉丁语、葡萄牙语，以及西班牙语写成的。

虽然亨利的作品质量并不怎么样，但是仍有许多女性被他吸引，也许是因为他比较老于世故。这些爱慕亨利的女性甚至会到监狱里来探望亨利。

亨利的左侧额头上有一条两英寸长的伤疤，据他自己称，这道伤疤是1862年被一位反叛的骑兵砍伤留下的（这一刀还砍伤了亨利右手的指关节）。此外，亨利的左手腕背部还有一个文身，图案是“两面三色法国国旗，以及十字交叉的杖，此外还有一个船锚和盘绕的绳索”。㊟

亨利留下的谜题除了他在狱中写下的密码以外，还有他的真实身份。亨利承认，他在埃塞克斯所用的名字只是一个化名，但是在搬到埃塞克斯之前，他在费城所用的名字也是亨利·德博斯尼斯。那么，这个假名到底已经使用了多久呢？他到底为什么要使用假名呢？这些问题亨利都没有回答。另外一个谜题是，有人给狱中的亨利送来了三件行李，这三件行李的寄送人不明，但是从行李的内容判断，送行李的人似乎想要帮助亨利。这三件行李中有两件里含有枪支、刀具、牛角制火药桶，好在监狱的工作人员及时发现并将它们没收，因此亨利并没有拿到。亨利只拿到了第三件行李中的物品，包括个人文件、密码、诗歌，以及他自己绘制的素描画。在狱中等待庭审的过程中，亨利又创作出更多密码、诗歌和素描画。

究竟是谁给亨利送的这些行李？根据调查，亨利是孤身一人来到埃塞克斯的，并且在埃塞克斯也只和贝齐一人比较亲近。显然贝齐的女儿不会想要帮助和安慰亨利。那么还有谁能拿到亨利的个人文件呢？

亨利的密码都相当长，这说明他想要隐藏的信息数量很多。亨利声称，这些文件中隐藏着他的真名，但是他并没有指出究竟在哪一页上。亨利的这一声明并不意味着他的真名一定藏在加密文字中，也有可能他的真名就在他用英语明文写下的自传性文字细节中。不管怎么说，在破译密码时，密码的上下文都非常重要。因此，我们有必要看一看在亨利写下的文献，以及在他接受采访时的发言中，到底有哪些关于他的信息。但是，在研究这些内容之前我们一定要记住，这些信息都可能是亨利编造出来的虚假信息。以下是亨利给《邮报》（*Post & Gazette*）提供的信息：

> 我1836年5月16日出生于葡萄牙的贝伦市我叔叔的种植园，距离里斯本只有几英里，在塔霍河的岸边。1836年11月，我随父母离开那里去了法国。1838年4月，我们又迁往格雷斯港，并在那里住到了1839年1月。1839年1月，我和父亲去了吉罗蒙特。1843—1845年，我在吉罗蒙特的公立学校上学。1845年6月，我离开那里，到贡比涅学院上学，直到1847年9月。1848年2月—1850年10月，我参加了麦克卢尔的北极探险队。1852年1月到1853年，我在巴黎生活。1853年5月到1854年，我被大学院录取。1854年6月到1856年，我和我父亲以及我的一个兄弟自愿入伍，参加了克里米亚战争。1856年7月，我被滨海省圣布里厄克神学院录取，并一直在那里学习到1858年1月（我接受的培训是如何成为天主教神父！）。1858年2—8月，我在巴黎高等师范学校学习。[注]

也就是说，根据亨利提供给《邮报》的上述生平信息，他22岁的时候还在巴黎。但是，这与此前他向警方提供的一份简要生平信息的内容相矛盾。亨利在给警方的这份声明中说：

> 我46年前出生于葡萄牙，在巴黎接受了如何成为天主教神父的培训课程。我在大学里待了两年，然后离开巴黎来了美国，因为我决定皈依美国的圣公会。当时我大概17岁。4个月之前，我从费城来到埃塞克斯，我是自己开船来的。我一路经过了纽约、哈得孙河、尚普兰运河和尚普兰湖。我来这里是为了我的事业——当一名画家。我6月8日与死者结婚。我是无辜的——我并没有犯你们控告我的罪行。[注]

亨利告诉警方的这个版本会不会更接近真相呢？在报纸对亨利的访谈中，接下来亨利叙述了更多关于旅行和冒险的经历（有可能是虚构的）：

1859年，我自愿入伍参加意大利战争，在麦克马洪手下效力。1859年8月，我在热那亚登船前往中国，在八里桥伯爵手下效力。1860年，我在北京生活。1861年8月，我在墨西哥生活，是巴赞的手下。巴赞叛变以后，我加入了墨西哥一派。1862年6月7日，我在德尔帕斯阿米德霍受伤，当时我是洛佩斯手下的游击队队长。1863年2月，我在美国自愿加入宾夕法尼亚第四军团，在麦金托什手下效力。1863年7月，我在葛底斯堡，头部和左手受了剑伤。1864年3月，我回到法国。1864年5月我和朱迪丝·德马雷小姐结婚。1864年7月—1867年2月，我参加了极地探险队，在弗兰克上尉手下工作。1867年2月，我回到罗马。1868年3月，我去了巴黎，然后在1868年6月，我到了纽约。我和奥塞奇部落的人一起沿着加拿大人河去了坎维尔溪的印第安人领地。1869年6月，我又回到纽约。1870年，我和600个美国人一起自愿参加了普法战争。(注)

亨利在写下上述经历时加了一些批注，但报纸的这篇报道里并没有登载出来。其中一条批注表明，亨利于1870年10月改了名字，然后被送往了罗纳河的军队。在报纸上登载的信息中，亨利1870年10月的经历如下：

在法国，我10月在布尔巴基将军麾下效力，10—11月在德比瑟罗勒将军麾下效力。12月在奥坦，我是德比瑟罗勒将军麾下的上校，参加了一些小型战役。12月15日凌晨3点，我们把普鲁士人赶出了尼伊苏博恩，并且占领了该地，俘虏55人，缴获了武器和物资。12月16日，我们在奥坦游击战中占领了路和石桥。11个人和两匹马牺牲，我们只能退回丛林中，又损失了4人。12月19日，我们在奥坦路上袭击了先锋部队，杀了4个普鲁士人、俘虏7人，8个法国人被杀。12月28日，我们追击普鲁士“死亡”轻骑兵分队，俘获1人，缴获5匹马、1车粮食。1871年1月1日，我们沿路进行了圣克劳德游击战；1月4日和5日，韦尔甘战役；1月6日和7日，大进军；1月8日，迈松东战役，布尔巴基将军麾下的所有部队和第四轻骑兵连一起在

城堡作战；普鲁士人伤亡惨重并撤退，俘虏1 800人，整个部队一直追击敌军到圣玛丽。1月12日，袭击蒙彼利埃高地，缴获7门大炮，俘获50人，死21人，伤48人，烧毁3辆车。布尔巴基将军经过蓬塔利耶路以及瑞士的莱维里埃退回瑞士。㊟

3月份，亨利上校回到了马赛。亨利上校一直待在马赛，直到圣尼古拉斯堡垒和守护圣母圣殿旁的警察局遭到炮击，以及马赛公社的首领加斯东·克雷米厄投降以后。接着，亨利上校带着他手下的400人回到巴黎——这400人中有一些是在凡尔赛自愿加入常备军的，还有一些是在圣克劳德自愿加入的。在巴黎公社期间，亨利上校和父亲一起住在巴黎，他手下有400杆枪，并且他拒绝把这400杆枪交给巴黎公社。因为他不肯参加巴黎公社，并且不肯交出手中的枪，克吕瑟雷将军和罗塞尔将军威胁要枪杀他，以及一个叫德勒克吕兹的人。亨利上校制作了一些木盒子，把他的枪放在这些木盒子里，并且藏在家中的地窖里，凡尔赛常备军进入巴黎时成功找到了这些枪。亨利上校被逮捕并送到凡尔赛，他在凡尔赛被判当日枪决。但是，亨利上校成功地从一个30人的步兵队手中逃脱，并且逃回了巴黎的父亲家。他从父亲那里拿了300法郎，然后乘车去了比利时的布鲁塞尔，并在那里一直待到审判结果被推翻才离开。接着，亨利上校回到巴黎，并且于6月登上了开往纽约的辛布里亚号前往格雷斯港。他的妻子朱迪丝·德博斯尼斯于7月死亡，遗体被送回法国，葬于她的家族墓室中。朱迪丝的父亲陪同朱迪丝的遗体一同回了法国。除了一小笔有利息收益的钱款以外，朱迪丝把所有财产都留给了孩子们。㊟

我认为，在上面这段文字中有一点非常奇怪：亨利完全没有提到他的妻子朱迪丝的死因，但他却详细地描述了朱迪丝的财产分配问题，似乎财产对他而言比死因更加重要。注意，在亨利的叙述中，朱迪丝没有给亨利留下任何财产。一份报纸的报道称，朱迪丝被发现在纽约市的一条河里溺亡，而亨利是该案的嫌疑人。然而，亨利丝毫没有提到这一点。亨利的个人生平继续如下：

此后，亨利·德博斯尼斯每年春天都会回法国与家人共度一两个月。他有两个孩子——一个女儿和一个儿子。1883年2月，他的女儿17岁。1882年10月，他的儿子14岁。这一儿一女和亨利·德博斯尼斯的一个姐妹一起住在英格兰，他们接受英语、法语、西班牙语和德语的教育。亨利的父亲和子女都不知道亨利被捕了，就连亨利死了，他们也不会知道。亨利留下一栋房子，在他父亲死后，这栋房子将属于他的两个子女。1871年，由于纽约格兰德街上的一场火灾，亨利蒙受了9 000美元的财产损失。1872年8月，亨利去了加拿大。同年12月，他与他的第二任妻子塞莱斯廷结婚。1873年3月，他们搬去了基斯维尔。1873年4月，他们又搬到了埃塞克斯，并在该地一直住到1873年7月。接着，这对夫妇搬去了佛蒙特州的伯林顿，并在该地一直住到8月27日。1873年9月—11月期间，这对夫妇住在纽约；1873年12月至1875年11月期间，他们住在费城；1875年12月至1878年5月，他们住在奥马哈。1876年5月，亨利将农场留给他的兄弟照看，并与妻子一起搬去了加利福尼亚州。同年9月，他们搬去了布莱克丘陵，并在那里一直住到1877年10月。1878年5月，亨利出售了他名下的农场，并且于1879年6月搬回了费城。1879年10月至1881年5月，他住在特拉华州的威尔明顿。德博斯尼斯夫人（塞莱斯廷）1882年3月5日死于费城。(注)

在上面的这段自白中，亨利似乎再次因为篇幅所限而没有提到他第二任妻子的死因。这次，他的妻子似乎是死于饥饿。一个人怎么可能自己摄取足够的食物而让妻子活活饿死呢？这实在是一件相当可疑的事，但是亨利靠某种方法逃脱了怀疑而并没有被逮捕。当亨利的第一任妻子朱迪丝在河里溺亡时，亨利也同样没有被警方逮捕。

此外，亨利在他的这番动机不纯的自白中还省略了另外一个事实，那就是：在塞莱斯廷死后不久，亨利就雇用了一个名叫伊丽莎白·布朗的管家来替他做饭。是的，你没有看错，虽然他的妻子刚刚被饿死，亨利却有足够的钱雇一名厨娘！

接下来，亨利的自白转向了他的第三任妻子。正是因为第三任妻子的死亡，亨利才最终受到了法律的制裁，虽然他本人从未承认过自己有罪。

> 1882年5月1日，亨利出售了他在格林尼治点的房产，并且搬回了埃塞克斯。1882年6月8日，亨利与伊丽莎白·韦尔斯结婚，并于同年8月1日因涉嫌谋杀妻子而被捕。1883年3月7日，亨利被判处死刑。1883年4月27日，亨利被执行绞刑。[注]
>
> 从1871年到今天，我的历史被毫无保留地记录下来。在我的年表上，我在每一处停留的情况，我都有相关文件可以证明。这些文件在我的行李中，和其他家庭文件放在一起（如果它们还没有被偷走的话）。我不断在各地旅居，因此在这篇陈述中我没有办法一一写完我的所有经历。为了完整讲述我的家族故事，我决定保留我人生中的一些片段。在这里，我只能向你们讲述关于我的旅程，以及关于我的职业的只言片语。[注]

显然，在这段话中亨利提到的行李并不是指他在狱中的行李。因为如果他指的是在狱中的那件行李的话，他应该很清楚这件行李是否已经被偷走。因此，亨利所指的行李可能是某件留在他死去的前妻的房中的行李。如果真是这样，那么现在想要去查看这些文件来证实亨利自白中的种种细节显然为时已晚。贝齐的家人并没有像亨利所害怕的那样偷走这些文件。在贝齐被谋杀以后，她的家人把这些文件与亨利的其他物品一起销毁了。因此，现在我们能看到的只有亨利在报纸上发表的这篇自白。

> 我是一名还不错的装饰画画家，我曾在纽约、费城、芝加哥、新奥尔良、布法罗，以及奥尔巴尼工作。但是我的捕兽水平比绘画水平更高，我也非常热爱运动。我对运动的热爱超出了我对其他任何职业的热爱。我和我的叔叔一起以商人的身份去了印第安人的领

地，我独立谋生，并且生活得非常好。然而，由于我遇上了一些事故、疾病和死亡，我又变得非常贫穷。我从不在同一个地方长时间停留，因此我没有朋友。如果我喜欢去酒吧，并且愿意花钱为任何跟我一起工作的人买一杯酒的话，我一定会有很多朋友的。只要你有钱，你就会有好朋友，然而一旦你的钱花光了，你的好朋友也就不见了。我从来没有这种朋友。我从来没交过坏朋友，也从来没有侵占过他人财物。如果我变穷了，那也是因为疾病的原因。我不会说我是世界上最好的那类人；不，但是我也从来没有伤害过任何人。关于我的虚假中伤比其他任何事情都要多。

亨利·德博斯尼斯受过良好的教育，能说6种语言，并能流利地用其中的5种语言阅读和书写。他的绘画水平相当高，可以称得上是一位不错的画家。但他并不像人们以为的那般清白。他说，他知道那些赞美之言的价值，他感谢埃塞克斯县的人们对此事进行了公正的判断，也感谢他们在他被捕以来为他树立起良好的个人形象。但被捕这件事并不会伤害他的名声，也不会伤害他的家族——因为人们从来没有机会知道他的真正姓名。他说，他已经准备好走向坟墓，死亡完全不会令他感到害怕。

现在，他养了若干动物，这些动物组成了一个动物园——一个会哭的小婴儿、一头会踢会叫的驴、一只会吠的狗、一只会咩咩叫的山羊、一只会叫的乌鸦、一只会打鸣的公鸡，这些都可以在詹金斯先生旅馆（指监狱）里免费看到。

关于他一生的秘密将会在他死后被印刷出来。

这篇文章的结尾写道：

以上内容摘自亨利·德博斯尼斯的手稿。德博斯尼斯说，他会在下一期继续讲述更多的个人历史。关于上文中提到的动物园，德博斯尼斯做了如下解释：他是一个非常优秀的声音模仿者。每天下午，当他被锁在牢房中的时候，他便会开放这个“动物园”，完美

地模仿若干种动物和鸟类的声音。注

在亨利的一幅绘画中画了一块墓碑，墓碑上写着："给亨利·D.德博斯尼斯——第二萨托里军团上校——国际社会1882。"注但是，在亨利的自传中，从来没有提到"第二萨托里军团"。

在另一篇陈述中，亨利更详细地讲述了自己的生平。如果这些细节是真的话，也许可以帮助我们找到亨利的身份。

> （关于与朱迪丝婚后生的两名子女）他们接受了英语、法语、德语以及西班牙语的良好教育。两个孩子每年各有600美元的年金，这是母亲留给他们的遗产每年产生的4%的利息，此外法国巴黎还有他们的产业。亨利的女儿和儿子对此桩惨案以及他们的父亲被判死刑一事一无所知。亨利的家族成员也永远不会把这些事情告诉这两个孩子。亨利的一位兄弟E. A. 德勒特纳克·德博斯尼斯住在美国靠近内布拉斯加，或者得克萨斯的某地。亨利在内布拉斯加州时，曾经将一些产业托付给这位兄弟照管。此后，亨利于1875年1—5月期间搬去了加利福尼亚州。1876年9月，亨利搬去布莱克丘陵，并在那里一直住到1877年10月。亨利曾在奥马哈出售过一个160英亩的农场（该农场是亨利名下的产业，获得600美元的现金）。接着，亨利与他的妻子一起搬回了费城。在纽伯格，亨利购买了一艘渔船，并且以每月20美元的价格将这艘渔船租给了新泽西州大西洋城的一个机构。在特拉华州的威尔明顿，亨利花157美元现金从马丁内斯·库利先生手上买下了一艘多帆单桅小船。该船被租给卡姆登的H. C. 哈姆伦。这些船只都是给亨利的儿子购置的。在捕鱼季节中，亨利的儿子每月会从这些船只的租金中收到50美元的收益。在夏季，这些船将蔬菜运往不同地方的市场，这些地方包括费城、罗切斯特，以及纽约州的卡姆登。注
>
> 关于我四处旅居的经历以及我在这个国家的职业，在这里我只能非常简要地描述，这么做是考虑到我的家族名誉以及我家人目前

的情况，而不是因为我过去的生活有什么见不得人的地方。不是这样的。然而，我的这些经历只应该被我的家人和朋友知晓。让我个人来承受这种堕落，而不要给我的家族带去任何不好的名声，对我而言这已经够了。在这个世界中，我的家庭成员永远不会知道我的堕落！埃塞克斯县的许多好奇而无知的农民都在说我的坏话，并且编造各种各样关于我的故事，然而他们却根本不知道我的名字和我的亲属关系。这样的人在各种地方编造谣言，他们事实上比罪犯更坏。哪怕数以千计的人把我包围，我也不害怕，即便有一万个这样的人攻击我，我也不会感到害怕。我将平静地躺下，安眠入睡。㊟

在亨利的自传的第一段中，他称自己曾在法国瓦兹省的一个名为吉罗蒙特（Giromaunt）的村庄里居住和上学。法恩斯沃思对这个地名进行了研究，发现这个村庄名称的拼写已经变成了“Giraumont”。亨利有时候还把这个地名拼写作“Giromond”，这就把事情搞得更加混乱了。关于自己在吉罗蒙特的生活经历，亨利做了以下的描述：

这一页描述了德博斯尼斯家族在1850年居住的地方。这处居所，或称城堡，是由米多勒·D.德博斯尼斯先生于1740年建造并装修的，其规模和装饰都充分反映了德博斯尼斯家族的品格和财力。该居所建在一个椭圆形的平原上，这个平原位于一座山的顶部。其东边和北边是大山，南边和西边能看到延绵几百英里的草原，那是世界上最险峻、最美丽的地平线之一。在住所的南面是大片的风景，没有任何遮挡，一直能望到天边。在地平线处，自然似乎处于永恒的安眠之中，这仿佛是为了和西部粗粝而涌动的宏伟景色形成最强烈的对比。在广阔的视野中，以及在南面和北面，零星地有一些孤立的山峰，它们使这片迷人的风景更富有活力和多样性。在这些山峰中，有一座南克莱罗伊山——他在笔记中对南克莱罗伊山做了非常有趣的描绘。站在这个地方，哲学家会习惯于享受这样的风景，并欣赏大自然造物主的伟大，同时他还能看到远处若隐若现的山峰，看见树木的摇动，以及从山顶上观赏天球宏大的运动。爱国

者可以向下俯瞰，欣赏一望无际的世界，并在心中念着这就是他出生的祖国；他也可以向上仰望，欣赏开阔的天穹，那似乎就是他将去往的天国——这样的风景会时时提醒他肩上的责任。㊟

走向西南的塔楼时，访客会情不自禁地驻足观看那震人心魄的宏大全景。然后走进门厅，在这里，即便是此前对这家人一无所知的人，也会立刻意识到这不是一处普通人的住所。访客眼前展开的是一个极其高大的门厅，这里没有任何俗气或不必要的装饰。访客的前方、右边、左边、周围，目之所及都是与科学有关的有品位的物件。这些物件的分类和陈列方式让它们展现出最好的效果。访客的一侧是一排雕塑，这些雕塑的排列方式能让人一眼看到艺术史的演进。走过门厅以后，访客被引入一间高雅的客厅，在这里，西侧美丽的风景再次跃入他的眼帘。客厅里挂满了画笔所能画出的最出色的杰作——来自全国各地、各个历史时期的历史画作，画的都是最惊人的物件。此外，还有名人和爱国者的肖像画——既有美国的，也有欧洲的——以及大量的浮雕和团花装饰。很少有哪处住所能像D.德博斯尼斯先生及其家人出生的这座城堡这么迷人和宏伟。这里还有一个美丽的花园，从花园里能够看到山峰、河流和峡谷。花园的一部分是一个精心维护的草地滚球场。它在城堡的一侧，球场和一条公路平行，中间被一排树篱隔开。㊟

在这座城堡中，最好的房间属于我的父亲、母亲和我的姐妹们。而我住在一楼厨房隔壁的一个小房间里。透过我房间的一扇窗户，就能够看到外面的草地滚球场。㊟

有一天晚上，天气异常闷热。按照我父亲的习惯，我们很早就就寝了。由于我的房间里过于闷热，我不但无法入睡，甚至根本不能休息。很不舒服地翻来覆去了很长时间以后，我决定起床。我穿上衣物，打开窗户，然后爬到了外面的草地滚球场上。那个夜晚是极美的，一轮满月散发着灿烂的光芒——事实上那个夜晚简直就如白昼一般明亮。在花园里散完步以后，我又回到了草地滚球场，在一颗布满了藤蔓植物的美丽乔木下坐下。夜晚的空气柔软、甜美而凉爽，所有景物都让我感到沉静和愉悦，只有远处瀑布的水声会打

破周围幽深的寂静。当我尽情享受着美丽的风景时，村里的钟敲响了一点钟的钟声，此时我觉得自己听到了马蹄和车轮不断驶近的声音。很快，我的视野中出现了一辆马车，缓慢地沿着公路驶来。由于我头顶的这棵树在草地滚球场的另一侧，所以我可以在明亮的月光中清晰地看到那是一辆大型的家庭马车。这属于乡绅常坐的马车，通常会由两匹又高又胖的马拉着，而随行的车夫和男仆穿着制服、戴着三角帽。马车很快过了转角，我以为这辆车会向村里驶去。然而，事实并不是这样，这辆马车立刻停了下来。我听到车门打开的声音，还听到有人走下马车、走向城堡。“夜里还在赶路的旅人，”我想，“你们来投宿也是没有用的，我们肯定不能接待你们。”然而，显然我误解了这群人的意图。他们并没有走向城堡，而是走向了城堡的大花园。这群人站在了草地滚球场距离城堡最远的一端，那里的树篱非常稀疏和薄弱。这群人中的一个人立刻穿过了树篱，往草地滚球场走了几步，然后停下来认真地看了看周围。由于我是在军人中长大的，所以我对所有军队的制服都非常熟悉。因此，我立刻认出了这群人的穿戴：巨大的有金色花边的三角帽，蓝色和绿色的斗篷，过膝长靴和马刺，以及一个沉重的……㊟（也许后面还有一页，但已经遗失了）

除了以上这些内容以外，亨利还描述了他的叔叔莫里斯·德博斯尼斯（Maurice Debosnys）上尉，他的儿子死于一次决斗。既然亨利的自白中有如此丰富的细节，为什么没有任何人能够确定亨利的真实身份呢？也许某位身在法国的读者能猜出亨利究竟是谁吧！

亨利对他的总体生涯，尤其是对他的早年境况做了非常华丽的描述。但这些描述与费城一份报纸上所登载的情况形成了强烈的对比。在亨利被捕以后，这份报纸刊文描述了亨利在费城的生活情况。

人们说，德博斯尼斯是一个不负责任的懒汉，他在附近四处游荡，直到饥饿迫使他不得不干些体力活谋生。其实如果他愿意的话，他随时都可以在油坊里找到活干。法国社团留有一份记录，其

中记载了所有发放求助钱款的情况。这份记录显示，1878年12月该社团曾给亨利·德布瓦斯尼（Henri De Boisnys）和他的妻子发过2美元的救济款。从1878年12月一直到1882年3月9日他的妻子塞莱斯廷去世，德布瓦斯尼的名字经常出现在这份记录中，也就是说他时常到法国社团领取救济款。[注]

事实上，亨利的罪状远不止四处闲逛、不务正业这么简单。亨利是一名谋杀犯。如果他的前两名妻子也是被他所杀的话，那么他已经可以被称为一名连环杀手了。然而，与亨利有关系的谋杀可能还不止这几起。亨利在监狱中向警方供认，9年前他曾在埃塞克斯县短暂地居住过一段时间，并且他提到了一个叫亨利·勒迈尔的人，此人在那段时间失踪。亨利在狱中向警方提供了谋杀亨利·勒迈尔的嫌疑人的名字。埃塞克斯县的谋杀犯并不多，如果亨利在狱中恰好想要帮助警方侦破另外一起谋杀，这未免也太巧合了。因此，除了谋杀一名或多名女性以外，亨利可能还曾经谋杀过男性受害者。也许，在狱中等待审判的时候，亨利故意向警方提起了这件陈年旧案，以此来嘲弄警方，并给自己找些乐子。

在这里，我必须再次向读者强调：我们并不知道亨利的自传中究竟哪些是事实，哪些是虚构的情节！然而，对于亨利的故事的结局，我们却知道得非常清楚。1883年4月27日，由于谋杀贝齐的罪名成立，亨利被绞刑处死。亨利“声称”，在行刑的时候，他看到自己的兄弟挤在围观的人群中观看了他死亡的场景。

在亨利被执行死刑以后，有报道说他的整个身体都布满了文身，但并没有提供这些文身的细节。似乎“那个时代的本地媒体认为文身过于露骨，不宜在报纸上公开”。[注]

在前文中我们已经提过，在亨利入狱以后，许多女性被他吸引，并且到监狱中探望他。在被执行死刑之前，亨利将他的大部分手稿和插图交给了其中一位来探监的女性。这位女性将亨利的这些物品秘密保存了

30年。1917年，她去世，她的孙女内莉·特纳（Nellie Turner）发现了这些文件，但只是继续妥善地保存它们，而没有采取其他任何行动。最终，特纳女士把这些文件借给了她的女儿。1957年，报纸上出现了关于亨利一案的文章，于是特纳女士就把这些文件从女儿那儿要了回来，然后写信给报纸，提到她的祖母告诉她的关于亨利的故事。此外，特纳女士还开始接洽对这些文件感兴趣的博物馆。最终，她找到了伊丽莎白镇的阿迪朗达克历史博物馆。今天，这些文件仍然保存在阿迪朗达克历史博物馆中。其他一些拥有亨利的文件的人也同样把他们手中的文件交给了阿迪朗达克历史博物馆。一部分亨利的文件直到最近这些年才成为阿迪朗达克历史博物馆的藏品，比如，来自某位“泰勒夫人”的文件直到1991年才成为该馆的藏品。

也许破译亨利创造的密码能够带给我们一些关于亨利身份的线索。在破译这些加密文件时，最可能产生突破性进展的可能是一首加密诗歌。

这首诗的每两行诗末尾的符号都相同。如果这是一首普通的诗，这种情况是很合理的。但是，如果诗歌的每两句末尾押韵的话，两句通常不会只有最后一个字母是相同的。一般来说，押韵的两句诗末尾的最后两个或者多个字母都可能是相同的，然而在亨利的这首诗中却没有出现这样的情况。只有“[illegible]”（第15行和第16行）和“[illegible]”（第17行和第18行）例外。

上述证据证明亨利的密码很可能是一种替代式密码。并且，我们有理由相信，在这套密码中，每个符号可能代表多个字母。比如，出现在第3行和第4行中的符号“Ẋ”有可能代表两个字母，“.”代表一个字母，而“X”代表另一个字母。+和O也可能分别代表不同的字母，因此第13行和第14行中出现的符号“[illegible]”也代表两个字母。

在亨利的这首诗歌中，“[illegible]”这个符号有时也会颠倒着出现，这说明这个符号代表的两个字母可以以两种不同的顺序出现。在英语中，一个常见的例子是ER和RE。而另一些双字母组合中的两个字母的顺序则不

能颠倒，比如英语中只有QU，但不会出现UQ这种组合。

如果能找到其他类似的密码，上述破译思路就能获得更多支持的证据。事实上，亨利确实声称他的密码在欧洲曾被广泛使用。虽然我找不到一种至今仍在使用的和亨利的密码完全一样的加密系统，但是其他密码有着与亨利的密码类似的特点，因此我们有必要对这些密码稍微研究一下。

第一种与亨利的密码类似的密码叫作“科皮亚勒密码”（Copiale ciper）。一般认为，科皮亚勒密码出现的时间大约在1740—1780年。1970年，这种密码在东德的一座图书馆中首次被发现，但是它们直到2011年4月才被最终破译出来。破译科皮亚勒密码的密码分析家包括美国加利福尼亚州的计算机科学家凯文·奈特，[注]瑞典计算语言学家贝娅塔·迈杰希（Beáta Megyesi），以及另一位瑞典语言学家克里斯蒂亚娜·舍费尔（Christiane Schaefer）。他们要破译的科皮亚勒密码主要体现在一本书中，该书共有105页，包含75 000个字符。

在这本用科皮亚勒密码写成的书中，一共有90种不同的符号。因为每一个符号都前后一致地对应于同一种明文字母，所以科皮亚勒密码与加州的黄道十二宫杀手所用的密码（参见第4章）一样，是一种“同音字母替代密码”（homophonic substitution ciper）。

在科皮亚勒密码被破译以后，人们发现这本书描述的是18世纪德国共济会的一套仪式。有趣的是，成功破译科皮亚勒密码的三位密码分析家都不懂德语。

另一种与亨利的密码相似的密码是“福尔杰手稿”（*The Folger Manuscript*）中的密码。为了把福尔杰手稿介绍给美国国家安全局的工作人员，布伦特·莫里斯（Brent Morris）在不对外公开的保密杂志《密码学谱》（*Cryptologic Spectrum*）上专门发表了一篇关于福尔杰手稿的论文。这篇论文发表以后，美国国家安全局的另一位雇员唐纳德·H.贝内特（Donald H.Bennett）破译了手稿中的密码，并把破译结果也发表

在了《密码学谱》杂志上。后来，莫里斯和贝内特的上述两篇论文都被转载到了《密码学》（*Cryptologia*）杂志上。此外，莫里斯还写了一本关于福尔杰手稿的书。如果任何读者有兴趣全面了解阅读福尔杰手稿的详细方法，以及破译福尔杰手稿的过程，我强烈推荐大家阅读莫里斯的这本书。但是在本书中，我只打算简要地解释一下福尔杰手稿的破译方法。

在福尔杰手稿中，加密者用各种图形来替代字母以及常见的单词，然而这种密码却不是一种简单的MASC密码。在经过上述这重加密以后，加密者又把各个图形以多种方式组合起来。因此在最终的密文中，任意一个超过两个字母的单词都可以被加密成多种不同的形式。

为了验证我关于德博斯尼斯的密码的猜想，我联系了我能联系到的最合适的权威专家——布伦特·莫里斯。布伦特·莫里斯不仅发表过关于共济会密码的论文，还写过前文提到的关于福尔杰手稿的书籍，而且他还是美国国家安全局的一名密码分析专家，他的其他许多工作成果可能因为保密的要求而无法公之于众。此外，莫里斯还是共济会的第33级成员，并且是全世界发行量最大的共济会杂志《苏格兰仪式期刊》（*Scottish Rite Journal*）的主编。在莫里斯写给我的一封电子邮件中，他表达了与我类似的看法。他认为“德博斯尼斯密码看起来像是一种典型的共济会密码，因为德博斯尼斯密码也是由一些不连续的神秘符号构成的”。㊟

莫里斯进一步向我指出，还存在另一种尚未被破译的共济会密码。在《未解之谜（下）》的第9章中，我会向读者详细介绍那种密码。心急的读者可以直接翻到《未解之谜（下）》第9章，阅读第9章介绍的最后一种密码。

如果亨利·德博斯尼斯的密码确实是一种共济会密码，那么就产生了一个很自然的问题：亨利是否与共济会有某种联系呢？似乎亨利确实与共济会有关系，但是他和共济会的关系可能出了一些问题。作为这方面的证据，我想向读者指出以下事实：亨利总是把著名的共济会标志

（方矩和圆规）倒过来画。在亨利的那首加密诗歌的页面左上方空白处，就出现了这种图案。

法恩斯沃思也注意到了这一点，她写道：

> 除了在密码中画出的符号以外，亨利还用其他方式提过现代共济会。比如，在亨利的诗歌《可怜的亨利——我最后的旅程和我的告别》（Poor Henru — My Last Voyage and My Adieu）中，亨利写道：“为了我的儿子——他此时已被我留在身后，如同我生命的阴影一般，不再会被引入第一级（the first degree）。”这里的“第一级”是指什么呢？我猜测，“第一级”是指进入共济会的第一级。在某一份密码的末尾，亨利画了一个握手的图样，握手是共济会成员进入共济会第一级（又称“入门学徒”）时使用的一个秘密手势。这种秘密的握手手势被称为“波阿斯”（Boaz）或者“入门学徒石匠之握”（grip of an Entered Apprentice Mason）注。注

也许是为了给想要破译密码的人提供一些线索，亨利在加密诗的纸张背面把这首诗翻译成了希腊语。

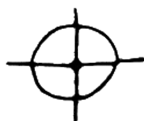
如果能把这些希腊语的单词和密码相互对应起来，就可以破译这个加密系统。然而，要想把这篇希腊语译文与密文中的符号简单地一一对应起来并不容易，因为密码所使用的语言可能是英语、法语、拉丁语、西班牙语、葡萄牙语，或者任何亨利能读写的其他语言。在这种情况下，密码的破译者必须先研究希腊语译文重新被翻译回原始语言（上述语言中的一种）的多种可能性，再把原始语言的明文与密码的密文匹配起来。虽然这个任务非常困难，但我仍然认为这是本书中最容易破解的密码之一。也许，我的某一位读者就能把这段密码从“未解之谜”变成“已解之谜”！

亨利所画的图中包含若干美丽女子的肖像。我们知道，亨利曾在狱

中画过贝齐的素描像，然而他画作中的其他女子的身份至今尚无法确定。这些女子会不会是亨利的前几任妻子呢？亨利写下的密码中是否有关于他前几任妻子死因的线索呢？这些密码中是否隐藏着亨利的真实身份呢？我相信我们很快就会知道这些问题的答案。

有些凶手像亨利一样用密码来记录不希望任何人读懂的想法或事实，而另外一些凶手，比如恐怖主义组织中的某些人，则会通过密码来和组织的其他成员共享信息和计划。也就是说，有一部分人能够读懂他们的密码。在21世纪的今天，恐怖主义者使用的密码复杂度各不相同。然而，在20世纪20年代，恐怖主义者使用的密码大多相对简单。

IRA密码（20世纪20年代）



汤姆·马洪（Tom Mahon）是一名原籍都柏林的医生和历史学家。2001年，他在都柏林大学学院的档案馆中做研究时发现了一批加密文件。这批文件是20世纪20年代恐怖主义组织“爱尔兰共和军”（Irish Republican Army，简称IRA）的成员写的。随着研究的深入，马洪发现了越来越多的加密文件。这些文件是由莫斯·图米（Moss Twomey）的家人捐赠给都柏林大学学院的，莫斯·图米曾于1926—1936年间担任爱尔兰共和军的总参谋长。

2004年，一直没有解开这些密码的汤姆·马洪终于决定寻求外界的帮助。在多方求助无果以后，马洪把这些密码交给了美国国家安全局。而美国国家安全局建议马洪求助ACA。ACA并不是另一个缩写为三个字母的美国国家机构，而是指美国密码协会（American Cryptogram Association）。在美国密码协会的官网上写着：该组织是一个“非营利性

机构，目标是推广密码分析这一爱好以及密码分析的艺术”。(注)马洪将文件中的6段密码发送给了美国密码协会。仅仅两个小时以后，詹姆斯·J.吉洛格利就回复了马洪，并且给出了密码的解法。双方的合作由此正式开始了！

我将马洪发现的其中一段密码复制如下。(注)这段密码的前面有一段未加密的英文，来自一位“琼斯先生”（Mr. Jones），这位琼斯先生的居住地在纽约，他是苏联人安排在此地的间谍，目的是为了帮助IRA筹集资金。这段密码的内容如下：

> 我的工作变得非常困难，我被要求集中精力尽快提供结果。我已经那么做了，但是它意味着：——
>
> OEOCH HOGNW TIWAT CEROS TDHOT NOLOO UGLAI AHUEI AMGVW NGTEE NOENI EREYI RLEWH NUAIO NLGDG FIHDT OTIST WEEIM PARDB KAROP HNGNA HEHDH HPMDT EDFTG OLNNO FENOP ARIYU NEESA TPRLB NAPKS WTMRW EIADA IIHV (164).

只要简单地统计一下这段密码中的字母频率，就会发现这里的字母频率与正常英语的字母概率非常接近。这意味着，密码中的字母并未做过替代处理，加密者仅仅改变了字母的顺序来隐藏文字的内容。这种加密系统被称为“换位重排密码”。在本书的第2章中，我已经向读者介绍过一些古埃及人和古希腊人使用换位重排密码的例子。当然，上面的这段换位重排密码要比古埃及人和古希腊人使用的稍微复杂一些。

在上面这段密码的结尾处，写着“164”，这个数字告诉我们密码中应该有多少个字符。如果密码密文中的字符小于164个，那么我们就知道这段密码中由于某种原因缺失了一个或多个字母。在这种情况下，收到密码的人会要求密码发送者重新发送密码。

要想读懂这段信息的意思，就必须把这段信息中的字母按照原始顺

序重新排列。为了做到这一点，收到密码的人必须使用一套密钥。在我们的这个例子中，密钥就是以下这串数字：

2 8 5 11 12 3 10 6 1 13 4 9 7

收到密码的人首先需要在纸上画一个表格，然后把密钥中的数字写入表格的第一行中。接着，他们需要把收到的这些字母按照一定的顺序填写到这些数字下面。完成第一步以后，就会得到以下结果：

2	8	5	11	12	3	10	6	1	13	4	9	7
								O				
								E				
								O				
								C				
								H				
								H				
								O				
								G				
								N				
								W				
								T				
								I				

第二步是填满数字2打头的一列，完成第二步以后得到如下结果：

2	8	5	11	12	3	10	6	1	13	4	9	7
W								O				
A								E				
T								O				
C								C				
E								H				
R								H				
O								O				
S								G				
T								N				
D								W				
H								T				
O								I				
T												

当这个表格中的11列被全部填满时，就会得到以下结果：

2	8	5	11	12	3	10	6	1	13	4	9	7
W	I	N	E	A	N	D	W	O	M	E	N	I
A	M	O	N	T	O	T	H	E	R	I	G	H
T	P	E	O	P	L	E	N	O	W	A	N	D
C	A	N	P	R	O	D	U	C	E	M	A	T
E	R	I	A	L	O	F	A	H	I	G	H	O
R	D	E	R	B	U	T	I	H	A	V	E	T
O	B	R	I	N	G	G	O	O	D	W	H	I
S	K	E	Y	A	L	O	N	G	A	N	D	S
T	A	Y	U	P	A	L	L	N	I	G	H	T
D	R	I	N	K	I	N	G	W	I	T	H	W
H	O	R	E	S	A	N	D	T	H	E	P	E
O	P	L	E	W	H	O	G	I	V	E	M	E
T	H	E	S	T	U	F	F					

接着，就可以从上述网格中直接读出明文的信息。我们给这段明文信息加上空格，信息的内容为：

WINE AND WOMEN. I AM ONTO THE RIGHT PEOPLE NOW AND CAN PRODUCE MATERIAL OF A HIGH ORDER BUT I HAVE TO BRING GOOD WHISKEY ALONG AND STAY UP ALL NIGHT DRINKING WITH WHORES AND THE PEOPLE WHO GIVE ME THE STUFF.

（葡萄酒和女人。现在我已经找到了正确的人，并且可以产出高级的材料了。但是我得带着上好的威士忌，彻夜与妓女们以及给我那些东西的人们一起狂饮。）

有些读者可能已经注意到，在填写上述表格中的字母时，有些列有

12个字母，而有些列则有13个字母。收到密码的人是知道这段信息的长度的，这里，信息的长度是164个字母。同时，收到密码的人还知道应该把这段密码分成13列。我们用164除以13，就得到12余8。这个结果意味着，有些列应该有12个字母，但是还有8列必须每列多添加一个字母。也就是说，靠左边的8列每列有13个字母，而靠右边的8列每列有12个字母。在解密这段信息之前，收到密码的人首先必须进行上述的简单计算，并且仔细数清楚每列中究竟应该放多少个字母。如果这些步骤都准确无误，最终就会轻而易举地解读出正确的信息。

创造这个密码的人完全不需要担心上面的细节。加密者只需要做三件事：一是画出正确的网格，二是将他想传递的信息以正常的方式写到这个网格中，三是按照密钥提供的顺序把网格中的字母逐列抄下来。完成上述三个步骤以后，加密者就可以得到一段密文信息。

当然，这段密码并不是专门写给吉洛格利的，因此吉洛格利并不知道形成密钥的这一串数字。他甚至不知道密钥中究竟有多少个数字。对于这种密码而言，我们无法仅从密文本身就迅速判断出究竟应该用多大的网格来进行破译，这个网格有可能有15列，也有可能只有5列，甚至有可能有20列。在破译了大量这类IRA密码以后，吉洛格利发现，IRA使用的网格的列数从6列到15列不等。由于对每一段特定的密码而言，吉洛格利并不知道网格的大小，所以他在破译这些密码的时候就要面对一重额外的困难。但是，这种挑战正是吉洛格利喜欢的！马洪和吉洛格利对他们的破译工作的结果做了以下的汇报：

> 最后，我们取得了相当大的成功。我们几乎破译了所有换位重排密码和替代密码，我们读出的信息甚至比密码原定接收者能读出的信息还要多，因为我们修正了密钥选择和加密过程中的一些错误。然而，仍然有少量的加密信息未能被成功破译，这其中包括一份来自大西洋彼岸的电报。在没有更多信息的情况下，我们无法破译这份电报所使用的加密系统。此外，还有一份弹药清单我们无法破译，因为仅通过这份清单的上下文我们无法获得这份弹药清单所

使用的数字替代系统。尽管如此，我们还是成功地破译了绝大部分的加密材料，这些材料的破译给了我们一个研究IRA内部情况的非常珍贵的机会。(注)

在所有的换位重排密码中，只有一条未能被成功破解。

这段密码的加密者在加密的过程中很可能出了某种差错。事实上，在这段信息的开头处写着52这个数字，也就是说这段密码中应该有52个字母，然而事实上这段信息中只有51个字母。

吉洛格利写道：

为了破译这段密码，我尝试了各种方法，比如逐一把缺失的字母放在52个可能的位置上（或者假设这个缺失的字母不存在，即这段密码只有51个字母），但是所有这些尝试都没有取得成功。如果你破译了这段密码，请告知我们。(注)

如果读者想要尝试破译这段密码，我必须提醒大家注意以下这个事实：IRA换位重排密码有时会多出一道加密程序，即在表格中包含一列由无效字母组成的空列。下面这个小例子可以解释这个加密步骤的原理。在这个例子中，信息的明文为：

I have other interests. I’m a magician.

（我还有其他的兴趣。我是一名魔术师。）

假设我们的密钥是5 3 6 1 4 7 2，并且把数字6所对应的一列设为无效列，那么在加密的过程中，我们就会把字母以如下的方式填入网格中：

5	3	6	1	4	7	2
I	H		A	V	E	O
T	H		E	R	I	N
T	E		R	E	S	T
S	I		M	A	M	A
G	I		C	I	A	N

接着，我们在数字6下面的这一列中填入与信息无关的字母，但是要保证这些字母的频率大致与正常英语中的字母概率相一致。这些字母就是所谓的无效字母。比如，我们可以填入以下这些无效字母：

5	3	6	1	4	7	2
I	H	N	A	V	E	O
T	H	O	E	R	I	N
T	E	E	R	E	S	T
S	I	I	M	A	M	A
G	I	T	C	I	A	N

然后，我们就可以根据密钥规定的顺序逐列读出密文。密文是：“AERMC ONTAN HHEII VREAI ITTSG NOEIT EISMA。”但当破译者试图破译这段密码时，他们很可能会走上歧途，因为破译出的头几个字母是IHNA，这看起来并不像一段有意义的信息的开头。然而，密码的接收者却知道这个表格中从左侧开始数的第3列是一个无效列，因此他们便可以轻松地破译这段密码。

吉洛格利一共破译了312份IRA文件，因此如果读者能够破译出吉洛格利未能破译的信息，那真是一项相当了不起的成就。在吉洛格利破译出的这312份文件中，许多文件中包括不止一段密码，吉洛格利总共破解了1 300段IRA密码。

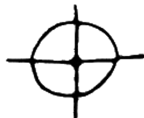
除了创造密码以外，IRA组织在密码的破解方面也曾经获得一些成功。马洪和吉洛格利写道：

> 在英国—爱尔兰战争期间，科克郡和凯里郡的IRA组织对警方使用的加密系统十分熟悉。1920年，在科克郡的IRA组织获得警方密码的关键字之后，破译了一封警方的快电，并且根据这封快电中的信息抓住了一位名为“奎因利斯克”（Quinlisk）的英国间谍，这名英国间谍被IRA组织枪杀，他的尸体被扔在一条水沟里。㊟

现在的我们可以把破译老密码当作一种消遣，然而在当年，破译这些密码的工作可绝对是生死攸关的大事！

在下文中，我将向读者介绍约翰·沃尔什（John Walsh）收到的匿名威胁信中的密码，显然，这些密码的破译工作也要认真对待。

蝎子信件



本书英文版的读者恐怕都很熟悉约翰·沃尔什。沃尔什遭遇了最凶恶的罪行，他6岁的儿子亚当（Adam）被人谋杀。面对这种悲惨的命运，沃尔什选择了反击——不是反击杀害他儿子的凶手，而是反击世间所有的凶手。沃尔什开始了一场针对犯罪行为的战役。在儿子被杀的惨剧发生之前，他并没有任何打击犯罪的技能或经验，此前，他只是一家酒店的市场营销经理。然而，在儿子被杀以后，沃尔什在伸张正义方面所取得的成就远远超过了许多接受正规刑侦训练的人。

约翰·沃尔什之所以能够取得如此巨大的成功，部分原因是他采取了一种创新的方式。用他自己的话来说，“我找到了一种不用枪就能抓捕罪犯的方式。”[注]通过在电视节目中播放通缉犯的信息，并吸引大量观众关注这些信息，沃尔什帮助警方获取了大量来自群众的线索。在沃尔什主持的《美国头号通缉犯》（*America’s Most Wanted*）节目播出1 000多集之后，2008年5月2日，该节目的官网宣布，该节目已经成功帮助警方抓获了1 000名通缉犯。[注]因此，如果一名在逃的罪犯不想被警方抓住的话，最理智的做法应该是不要被约翰·沃尔什的节目注意到。然而，却有一名疯狂的罪犯主动写信对沃尔什进行挑衅。

《美国头号通缉犯》节目公开了一桩针对他们节目的陈年旧案，15年前的1991年，节目主持人沃尔什收到了一系列匿名的威胁信件（“蝎子信件”），这些信件中包含经过加密的线索以及一些密码，信的作者宣称自己曾犯下多起严重罪行。美国联邦调查局（FBI）已经研究过这些信件，虽然FBI未能判断这些信件究竟来自谁，但是他们称，不是黄道十二宫杀手。信中所包含的密码目前仍然未被破译，节目组邀请广大观众帮助揭开这个谜团。

我将蝎子信件中的文字及密码部分复制于图5–1至图5–5中。在这些图片中我会插入一些分析。事实上，这一系列蝎子信件还包含更多内容，但是目前已经公布的只有以下这几部分：

I am your worst nightmare
coming true. My true identity is not known to
you yet, and hopefully will not be for a long
time. Your show is more exciting, interesting
and factual than any shitfalled movie or
series. I have recently moved into New
Jersey and began a new crime spree. I am
Currently responsible for 23 unsolved
crimes ranging from Arson to Burgulary to
Sabotage homicide and occasionally
everything in between. I strongly advise
that you keep this letter and start a
rather large file, since you will be hearing
from me again. I have enclosed a rather
difficultly encoded message containing
information that will prove ~~overly~~ rather
useful to you. This code took a lot of
time and effort to develop, in hopes
that it will defeat FBI and CIA code-
breakers. Anything you wish to tell me
or ask me can be conveyed to me on
your show.

SCORPION

图5-1 蝎子信件中的一页文字

图5–1中的信件内容翻译如下：

我将让最恐怖的噩梦成为现实。你还不知道我的真实身份，并且我相信在很长一段时间内你都无法发现我的真实身份。你的节目

比任何垃圾电影和电视剧都更加令人激动、有趣、实在。我最近搬到了新泽西州，并且开始了新的狂欢式犯罪。到目前为止，我已犯下23起未被警方侦破的罪行，这些罪行包括纵火、入室盗窃、破坏性凶杀，以及一些其他罪行。我强烈建议你保留这封信，并且准备一个大文件夹，因为我还会给你写信。我在信中已附上一条非常难解的加密信息，如果你能够破译这些信息的话，你会发现其中的信息对你而言非常有用。我花了许多时间和精力来创造这些密码，就是希望打败联邦调查局和中央情报局的密码破译师。如果你有任何问题想要问我，或者有任何信息想要传达给我的话，请在你的节目中告知我。

蝎子

虽然美国联邦调查局已经排除了蝎子信件的作者就是黄道十二宫杀手的可能性，但是读者不难看出，这些信件和黄道十二宫杀手的信件具有一定的相似之处。我相信这很有可能是因为蝎子信件的作者受到了黄道十二宫杀手所写信件的启发。

图5–2的这段密码一共有180个字符，因此我将这段密码称为“蝎子180密码”。这段密码的问题是，在这180个字符中，有155个字符仅仅出现了一次。即使根本不去尝试破译这段密码，我们也能够靠直觉猜到：由于没有足够的限制条件，破译者可以找到不止一种有意义的信息来与这些符号进行匹配。由于我们无法判断这么多种信息中究竟哪一种才是正确的解法，所以我们根本不可能成功地破译这段密码。但是，事实上我们没有必要被这种直觉吓倒。我们没有必要真的列出这些符号可能匹配的各种信息。因为从整体上来看，密码学家已经用数学的方法解决了这个问题。

Hi!
Remember me?



图5-2 蝎子180密码

在本书的第1章中，我已经简要地向读者介绍过信息的熵和冗余度的概念，这两个概念是由克劳德·香农提出的。然而，事实上对于熵和冗余度的概念还可以进行更加深入的挖掘，有大量书籍和文献专门讨论熵、冗余度，以及两者的应用。在这里，我只打算向读者介绍其中一个与我们已经讨论过的内容具有紧密联系的概念，就是“唯一点”（unicity point）。对于不同的系统而言，“唯一点”的定义也有所不同，但在任何一个系统中，“唯一点”度量的都是一个临界长度：在这个临界长度以下，密码存在多重可能有意义的解；而在这个临界长度以上，密码只有一个有意义的解。

为了理解有意义的密钥的数目如何影响“唯一点”的数值，让我们来考虑这样一段密文：“PNXX RJ”。如果这段密文是用MASC密码加密而成的话，那么这段密码就有多个有意义的破译结果——因为这段密码的长度太短了。这些有意义的破译结果包括：CALL ME（打电话给我），CALL US（打电话给我们），KILL ME（杀死我），KILL US（杀死我们）等。

然而，如果上面这段密文是用移位密码进行加密的话，那么可能的密钥的数量就会大大减少。事实上，作为移位密码，这段密码只有一种解法是有意义的（加密时向后移动5位，解密时向前移动5位）。在这种情况下，这段密文的唯一解法是KISS ME（吻我）。

上面的这个例子说明，密钥空间越大，唯一点也就越大。然而，我们仍然需要回答一个问题，那就是：唯一点的数值究竟以什么速率增长？事实上，唯一点数值增长的速率是相当慢的——它是以对数速率增长的。

然而，除了密钥空间的大小以外，还有另外一个因素也会影响唯一点的数值——这个因素就是信息所使用语言的冗余度。对于一种冗余度很高的语言来说，每个字母前面的字母会对这个字母的可能值产生很大

影响。而对于一种冗余度非常低的语言来说，之前的字母对后续字母的影响则非常低。语言的冗余度高，意味着这种语言的自由度更低，因此对于给定长度的信息而言，可能的有意义的解法也就较少。而当有意义解法的可能性较少时，通过不正确的密钥得到一条错误的有意义信息的可能性也就相应降低了。因此，当一种语言的冗余度较高时，用这种语言写成的信息的唯一点就会较小。

现在，我们已经知道唯一点的数值受到哪些变量的影响，下面就让我们来看一看唯一点的公式。如果我们用字母U来代表唯一点的数值，那么唯一点的公式可写作：$U = \log_2(K)/D$。其中K代表可能密钥的数量，而D代表这段信息中单位字母的冗余度。

如果我们想把这个公式应用到“蝎子180密码”中，我们就需要知道“蝎子180密码”的K值和D值。这段密码的D值并不难得到，在本书的第1章中我们已经给出了英语的冗余度，英语的冗余度大概是0.7左右（如果我们不把空格计作一个字符的话）。但是，在我们对这段密码还所知甚少的时候，如何能够计算出这段密码的密钥空间呢？在这段密码中，我们观察到一共有155种不同的符号。如果我们假设每种符号都可以代表任何一种明文字母，那么每一种符号就有26种选择，因此我们总共有26^{155}（约等于2.1×10^{219}）种可能的密钥。不过，这个巨大的数值中包含一些显然不可能成立的荒谬情况，比如所有符号都代表字母Z的情况。如果我们假设同音字母是均匀分布的，并且假设在“蝎子180密码”中所有的同音字母都出现了，那么每一个明文字母就大约可以对应于6种不同的符号。因此，我们可以给字母表中的26个字母分别安排6种不同的符号，不同排列组合方式的数量就大致相当于这段密码的可能密钥的数量。㊟对于可以分配给明文字母A的第1个符号，我们有155种选择；而对于可以分配给它的第2个符号，我们有154种选择（因为其中一个符号已经被用掉了）；对于可以分配给它的第3个符号，我们有153种选择。以此类推，可以分配给字母A的第6个符号就有150种选择。然后，我们再来考虑明文字母B。可以分配给字母B的第1个符号共有149

种选择，第2个符号共有148种选择，以此类推。因此，当我们按照这个思路进行到明文字母Z时，总共的选择可能性就等于从数字155一直乘到数字1。这个数值可以简写为155!，即150的阶乘。然而，事实上这种计数方法还多算了许多可能性。让我们来考虑一下分配给明文字母A的符号：第1种情况是把@、#、$、%、^、& 这几个符号分配给明文字母A，第2种情况是把&、^、%、$、#、@ 这几个符号分配给明文字母A，这两种情况有区别吗？显然没有。把同样的几个符号按照不同的顺序分配给同一个字母是不会产生任何实质性的区别的。由于把6个不同的符号分配给同一个明文字母的排列组合方式共有6! = 6×5×4×3×2×1种可能性，因此，对于明文字母A的可能分配方式我们多计了6！倍的可能性。同样，对于字母表中的每一个明文字母，我们都多计了6！倍的可能性。为了修正这个错误，我们必须把上一步的结果（155!）除以6！的26次方。也就是说，这段信息的可能密钥的实际数目是：

$$\frac{155!}{(6!)^{26}} \approx 2.45 \times 10^{199}$$

虽然这个结果已经比我们一开始估计的数值（2.1×10^{219}）小了很多，但这仍然是一个极大的数值。我们可以进一步论证上述估算中仍然存在一些不合理的假设。比如，在蝎子180密码中，不太可能出现字母表中的所有字母，字母表中的每一个字母都由6种符号来表示就更不可能了。更加合理的情况是：同音字母并非均匀分布。比如，在蝎子180密码中共有12种不同的符号代表明文字母E，而代表明文字母Z的符号则只有1种。我们可以继续修正假设，来不断降低对这段密码的密钥空间大小的估计，但是这个数值仍然会非常巨大，而且我们也无法确定修正后的估计值是否真的比此前的估计值更加精确。因此，我们不妨就停在2.45×10^{199}这个估计值上。

如果我把这个数值代入计算唯一点值的公式，我们就得到$U = \log_2(2.45\times10^{199})/0.7 \approx 946$。也就是说，如果密码的字符数小于946个，

这个系统就会出现多种可能的解法。这段密码中的实际字符数是180个，所以这段密码的字符数远远低于唯一点。因此，如果我们试图破译这段密码，就会得到数量巨大的多种解法，每一种解法都可能成立。由于我们不可能判断出这其中的哪一种解法才是写信人的原意，所以我们根本无法破译蝎子180密码。

然而，蝎子180密码中的许多符号具有一些几何上的性质。那么，把字母分配给这些符号的方式是否也具有一定的对称性呢？比如，如果我们找到了一种有意义的解法，在这种解法下“ ”= A，“ ”= E，“ ”= O（也就是带有*n*个点的方块表示第*n*个元音字母），并且许多其他符号也以某种规则与字母相互匹配，那我们就会有更强的信心确认出正确的解法。请读者注意，这并不说我已经确认了蝎子180密码中的元音字母——上述这种对应关系只是为了解释我的论点而举的一个例子。我的观点是：如果在一种解法中，符号和明文字母之间的匹配关系具有一定的逻辑性，且得到了有意义的结果，那么这种解法就很可能是正确的解法。这是因为，能把符号与明文字母以某种规则联系起来的密钥数量应该不多，这个较小的密钥数目就可以把这段密码的唯一点数值降低到密码的字符数以下。在《未解之谜（下）》的第9章中，我们会讨论共济会密码，到时候读者就会看到某些有逻辑的符号—密码匹配方式。

在尼克·佩林的“密码谜团”博客上，他提出蝎子180密码中有一种有趣的规律。这一规律并不是佩林本人发现的，他只是转述其他人的发现：

> 2007年5月，OPORD分析论坛上的用户“泰迪（Teddy）”指出，如果我们把S5（也就是我所说的蝎子180密码）的排列方式从12列转化为16列，那么在重排后的符号中，每种符号只会在同一个竖列以内重复出现（如果重复出现的话）。事实上，在重排后的符号中，除了第5列以外，其他所有列中都出现了一种或多种重复出现的字符。[注]

佩林还进一步猜测，重排后的这16列字符可能分别对应于不同的密码字母表。如果这一猜测正确的话，我们就有了破译蝎子180密码的另一条途径。

下面我们来考虑另一段蝎子密码。

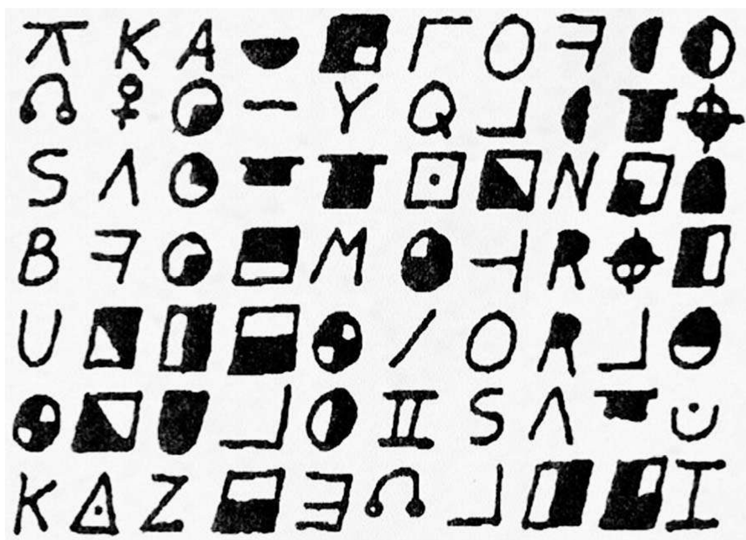


图5-3 蝎子70密码

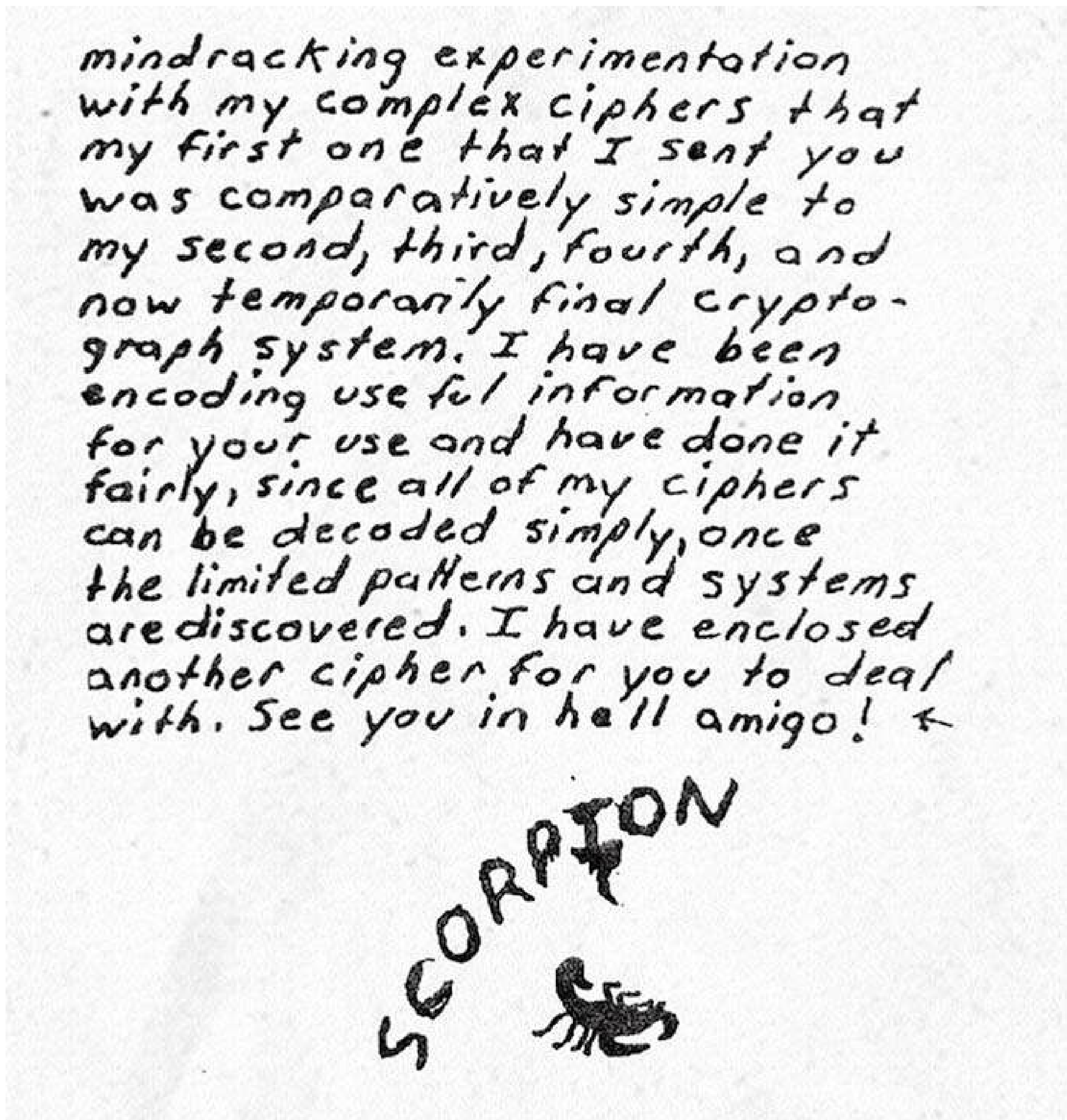
这段蝎子密码比之前那段蝎子密码要短。因为这段密码中共有70个字符，所以我把这段密码称为“蝎子70密码”。在这段密码中，我们也遇到了和前一段密码同样的问题。在这70个字符中，有53个字符只出现过一次，也就是说这个加密系统中的同音字符数量过大，因此这段密码的总字符数几乎肯定小于唯一点的数值。然而，在这段密码中同样也出现了一种规律。

此外，我们面前还存在这样一种希望：即使我们无法破译这段密码，我们依然有可能通过这段密码来确认凶手的身份，因为也许有人会通过这些密码的风格认出凶手。也许本书的某位读者正好认识一个曾用这种符号来加密信息的人。凶手是否具有足够的自控能力，能做到只在给约翰·沃尔什的信中使用这些符号呢？如果凶手还曾在其他地方使用过这些符号，或者凶手曾让其他人看到这些符号，那么我们就有可能从密码的风格中获得一些线索。

上面的这种希望看起来似乎很渺茫，然而，在现实中确实有过这样的先例。“大学炸弹客”[注]之所以会被警方抓住，就是因为他的弟弟认出了他的宣言的写作风格，并给警方提供了线索。在考虑到这样的先例之后，我认为寄希望于有人能认出蝎子所使用的加密方法也并不算是一种太过牵强的愿望。但是，不管怎么说，如果我们打算靠凶手的风格来把蝎子和某个具体的人联系起来，那么蝎子信件中的文字部分可能比密码部分更加有用。在图5–4和5–5中，我复制了蝎子信件中已经公布的其他文字。

intricate and difficult to recopy onto these cards. My style of handwriting on these cards is verry much altered, and controlled in order to throw off graphologists. I would much rather communicate vith you with letters sent between us but you and your over anxious associates would try to nail me even if I used a P.O. Box for a return address. This would create a rather messy situation since I do not plan to be taken alive if at all, and I truly believe in the use of superior firepower. This creates a problem for our communication since the only way I can communicate with you is by letter and possibly phone and your only safe medium in both of our best interests is your informative and helpful show. Consider this your second and definately last chance, since I will soon start collecting bodies for you, to prove that this is not a prank. Hopefully for you no one will expose themselves to me as an easy target for my ever growing anger before I get a chance to hear from you. I now realize with many hundreds of hours of

图5-4 你能认出这封信的风格吗？



mindracking experimentation
with my complex ciphers that
my first one that I sent you
was comparatively simple to
my second, third, fourth, and
now temporarily final crypto-
graph system. I have been
encoding useful information
for your use and have done it
fairly, since all of my ciphers
can be decoded simply, once
the limited patterns and systems
are discovered. I have enclosed
another cipher for you to deal
with. See you in hell amigo! ←

SCORPION

图5-5 为什么这些人都那么喜欢给自己取昵称呢？

……太过复杂难解而无法复制到这张卡片上。我已经对我的笔迹风格进行了控制以及大幅度改变，因此笔迹学家拿我没有办法。我很想与你互通书信，但是即使我不用真实的地址，而使用邮局信箱，你和你那些过于焦虑的同伴也一定会试图用我提供的回信地址

来抓住我。这会给我带来许多麻烦，因为我并不打算被抓住，尤其是不打算被活捉，而且我发自内心地认为应该使用更高级的火力。这就给我们的交流带来了一个问题，因为我能与你交流的唯一方式就是通过书信，也许还可以通过电话，并且我也只能与你一个人交流。对于我们双方的利益而言，最好的安全交流媒介是你所主持的节目，你所主持的节目既有丰富的信息量，又很有帮助。你应该把这视为你的第二次机会，并且这绝对是你的最后一次机会，因为我很快就会开始收集尸体，以此来证明这些威胁信并不是一个玩笑。你只能寄希望于没有人会主动把自己当成容易的目标暴露在我面前，在我听到你的回音之前，我越来越愤怒。在对我的复杂密码做了几百个小时的拷问头脑的实验以后，我现在认识到，我寄送给你的第一段密码相对来说比较简单，我的第二段、第三段、第四段密码，以及现在的最后一段密码的加密系统就要复杂一些了。我一直在通过加密的方法向你提供有用的信息，而且我的做法是十分公平的，因为只要发现密码中有限的规律和系统，就能够很简单地破解出这些密码了。随信附上另一段供你破解的密码。地狱见，朋友！

蝎子

针对这些文字内容，我们又要再次提出上面的问题：凶手的自控能力究竟有多强？在这些文字中，蝎子使用了一些奇怪的短语，比如“mindracking experimentation”（“拷问头脑的实验”) 和“See you in hell amigo!”（“地狱见，朋友！”，其中“朋友”一词是西班牙语）。那么，凶手究竟能否做到只在这些信件中使用上述短语，而在其他时候绝不使用这些短语呢？本书的读者中是否有人认识某个也喜欢使用这些短语的人呢？

直到2007年，蝎子的这些威胁信才被公之于众。因此，和一些更陈旧的案子（比如黄道十二宫杀手案）相比，也许到目前为止公众还没有足够的时间来为警方提供蝎子案的有用线索。此外，因为凶手写信的时间远远晚于黄道十二宫杀手写信的时间，所以这些信件的作者仍然存活

于世的概率也比黄道十二宫杀手仍然活着的概率要高很多。所以，虽然蝎子密码的唯一点分析结果并没有给我们带来令人鼓舞的消息，但这起案件的侦破工作仍有希望在未来取得某种进展。

也许，关于蝎子的身份，目前美国联邦调查局已经掌握了一些我们不知道的线索。蝎子信件中的其他文字和密码目前还没有被公布于世。也许在将来的某个时候，约翰·沃尔什会向公众公布更多关于蝎子的信息。

虽然这场打击犯罪的战争为沃尔什带来了巨大的知名度，但他并没有忘记自己的使命。他并不是那种愿意以嘉宾身份出现在“与星共舞”节目上的人。事实上，他曾表示：“我并不想出现在电视上……我也并不想帮警方追捕凶手，但是你知道，就像我的妻子经常对我说的一样，‘我们一定不能让亚当白白地死去’。”㊟

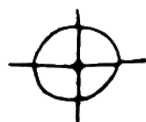
虽然沃尔什并不想成为名人，但是事实上他现在已经成了一个名人，而成为名人的代价之一就是会收到许多垃圾邮件。我相信，像大部分名人一样，沃尔什会完全无视他收到的大部分信件。即使他收到一些带有威胁或恐吓性质的信件，他也只会把这些信件交给警方而已。那么，对于我在本书中提到的这些蝎子信件而言，为什么沃尔什在等待了那么长时间以后，又选择把这些信件公之于众呢？在我看来，如果没有任何证据证明信中的这些说辞确有其事的话，在这么多年以后，沃尔什恐怕早已忘记了这些信件。由于我手头的所有线索只有被公之于众的这几封书信，所以我只能据此做出这样的猜测：一定有什么尚未公布的理由使得沃尔什认为必须认真对待蝎子的威胁。

在这封信中，蝎子声称他已对自己的笔迹做了伪装，然而，正如我在前文中所说的那样：蝎子是否也对他的文字做了伪装呢？在此，我再次恳请各位读者认真阅读这些信件，看看你是否能够认出蝎子的用词风格。正如沃尔什所说的那样：

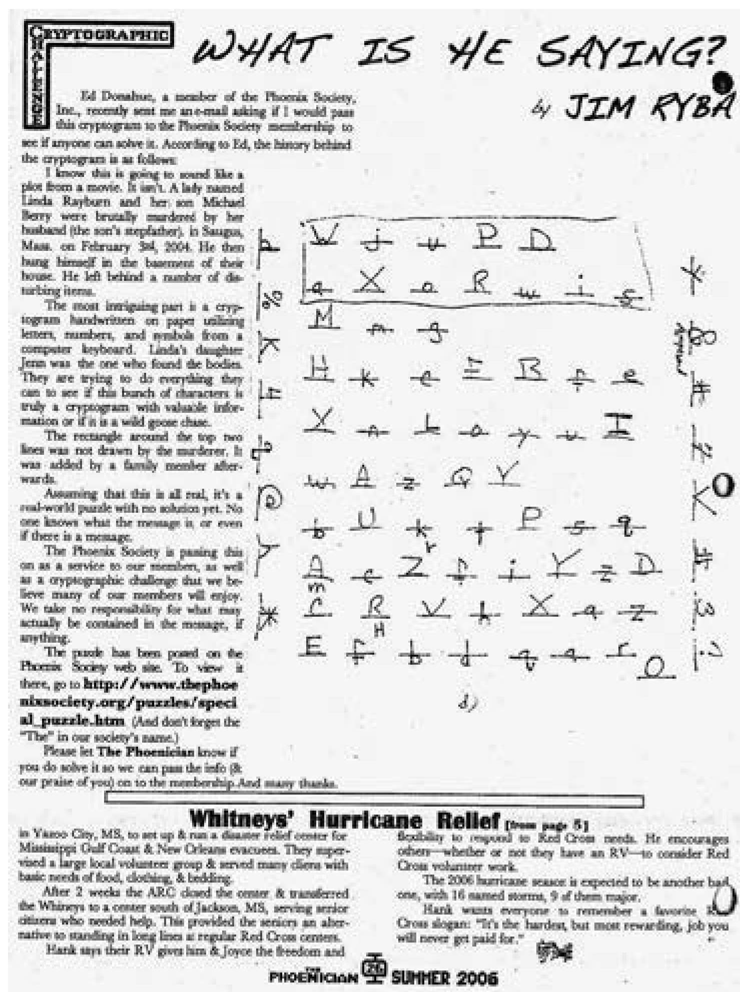
> 请记住，事情也许会因为你而变得不同。㊟

在有些情况下，虽然警方已经确定了凶手的身份，但是由于存在某些未被破解的密码，案件的某些方面仍然存在疑问。在下文中，我将向读者介绍一个这样的例子。

密码还是口令？



美国国家安全局有一个由退休人员组成的协会——菲尼克斯协会（the Phoenix Society）。这个协会除了举办各种活动以外，还出版了《腓尼基人》（*The Phoenician*）的黑白杂志。[注]该杂志的2006年夏季刊刊出了一段未破解的密码，据称这段密码与两年前的一起双重谋杀加自杀事件有关。我将《腓尼基人》杂志上的这篇文章复制在图5–6中。和《美国头号通缉犯》的观众一样，美国国家安全局的这些退休人员也愿意发挥自己的特殊技能来帮助警方打击犯罪。



CRYPTOGRAPHIC CHALLENGE

WHAT IS HE SAYING?

by JIM RYBA

Ed Donahue, a member of the Phoenix Society, Inc., recently sent me an e-mail asking if I would pass this cryptogram to the Phoenix Society membership to see if anyone can solve it. According to Ed, the history behind the cryptogram is as follows:

I know this is going to sound like a plot from a movie. It isn't. A lady named Linda Rayburn and her son Michael Berry were brutally murdered by her husband (the son's stepfather), in Saugus, Mass. on February 3rd, 2004. He then hung himself in the basement of their house. He left behind a number of disturbing items.

The most intriguing part is a cryptogram handwritten on paper utilizing letters, numbers, and symbols from a computer keyboard. Linda's daughter Jenn was the one who found the bodies. They are trying to do everything they can to see if this bunch of characters is truly a cryptogram with valuable information or if it is a wild goose chase.

The rectangle around the top two lines was not drawn by the murderer. It was added by a family member afterwards.

Assuming that this is all real, it's a real-world puzzle with no solution yet. No one knows what the message is, or even if there is a message.

The Phoenix Society is passing this on as a service to our members, as well as a cryptographic challenge that we believe many of our members will enjoy. We take no responsibility for what may actually be contained in the message, if anything.

The puzzle has been posted on the Phoenix Society web site. To view it there, go to **http://www.thephoenixsociety.org/puzzles/special_puzzle.htm** (And don't forget the "The" in our society's name.)

Please let **The Phoenician** know if you do solve it so we can pass the info (& our praise of you) on to the membership. And many thanks.

Whitneys' Hurricane Relief [from page 5]

in Yazoo City, MS, to set up & run a disaster relief center for Mississippi Gulf Coast & New Orleans evacuees. They supervised a large local volunteer group & served many clients with basic needs of food, clothing, & bedding.

After 2 weeks the ARC closed the center & transferred the Whitneys to a center south of Jackson, MS, serving senior citizens who needed help. This provided the seniors an alternative to standing in long lines at regular Red Cross centers.

Hank says their RV gives him & Joyce the freedom and flexibility to respond to Red Cross needs. He encourages others—whether or not they have an RV—to consider Red Cross volunteer work.

The 2006 hurricane season is expected to be another bad one, with 16 named storms, 9 of them major.

Hank wants everyone to remember a favorite Red Cross slogan: "It's the hardest, but most rewarding, job you will never get paid for."

PHOENICIAN SUMMER 2006

图5-6 《腓尼基人》杂志公布的一段未解开的密码

图中文章翻译内容如下：

他在说什么？

作者：吉姆·雷巴（Jim Ryba）

菲尼克斯协会的一位成员埃德·多纳休（Ed Donahue）最近给我发来了一封电子邮件，询问我是否可以将这段密码发给菲尼克斯协会的成员，看看有没有人能够解开这段密码。根据埃德的说法，这段密码背后的历史是这样的。

我知道这看起来像是电影里才会有的情节，然而这些都是真实

的。一位名叫琳达·雷伯恩（Linda Rayburn）的女士和她的儿子迈克尔·贝里（Michael Berry）被琳达的丈夫，也就是迈克尔的继父残忍地谋杀了。琳达和迈克尔2004年2月3日被杀于马萨诸塞州的索格斯。杀死母子二人之后，琳达的丈夫在他们家的地下室中上吊自杀。凶手死后留下了一些令人不安的物件，其中最奇妙的是在一张纸上手写的一段密码。这段密码由电脑键盘上的字母、数字，以及符号构成。发现尸体的人是琳达的女儿珍（Jenn）。他们正在尽一切可能想搞清楚这段密码是否包含有价值的信息，还是只是一个永远无法破解的恶作剧。

密码的前两行被圈出的长方形并不是凶手画的，这是他们的一位家庭成员在事后画上去的。

假设以上所有事情都是真实的，那么这就是现实世界中的一段尚未被破解的密码。没有人知道这段信息究竟是什么，甚至没有人知道这究竟是不是一段信息。

现在，菲尼克斯协会决定把这段密码发放给所有成员进行破解，这既是我们对我们的成员埃德提供的一项服务，也是一个我相信许多成员都会乐于尝试的挑战。如果这段密码中确实包含了某种信息的话，本协会不对这段密码中的信息承担任何责任。

这段密码已经被发布在了菲尼克斯协会的官方网站上。如果读者有兴趣仔细研究，可以前往以下网址：http://www.thephoenixsociety.org/puzzles/special_puzzle.htm。（请不要忘记本协会的名字前面有“The”这个单词。）

如果你解开了这段密码，请将解法告知《腓尼基人》杂志，我们将把你提供的信息（以及我们对你的赞美之词）传达给本协会的其他成员。在此表示万分感谢。

这里有一张更清晰的密码图像：

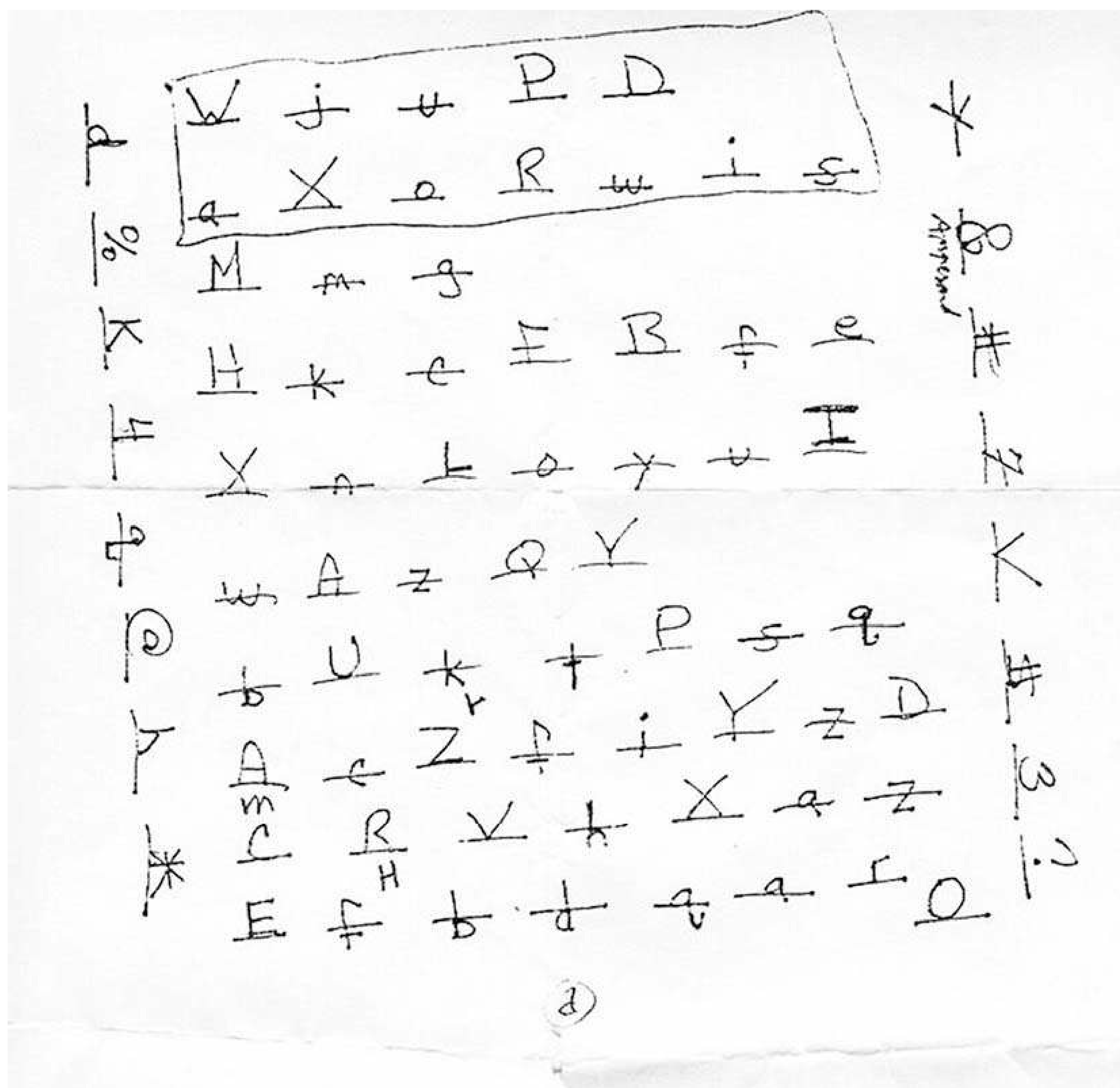


图5-7 与三人死亡事件有关的一段奇怪的密码

2006年早些时候，布鲁斯·施奈尔（Bruce Schneier）也在他的密码通讯/博客中提到了这段密码。我在取得了他的授权之后，将施奈尔博客中的相关内容转载如下：

2006年1月30日

现实世界中的一段手写密码

我常收到各种电子邮件，有时真的很诡异。每隔一段时间我就会收到类似的电子邮件：

我知道这看起来像是电影里才会有的情节，然而这些都是真实的。我的一个非常好的朋友琳达·雷伯恩和她的儿子迈克尔·贝里被琳达的丈夫，也就是迈克尔的继父残忍地谋杀了。

琳达和迈克尔被杀于2004年2月3日。(注)杀死母子二人之后，琳达的丈夫在他们家的地下室中上吊自杀。凶手死后留下了一些令人不安的物件，其中最奇妙的是在一张纸上手写的一段密码。这段密码由电脑键盘上的字母、数字，以及符号构成。发现尸体的人是琳达的女儿珍。珍是我非常好的朋友，因此我告诉她，我愿意尽我所能来搞清楚这段密码究竟是否包含有价值的信息，还是只是一个永远无法破解的恶作剧。

我完全不知道这封邮件中的信息是不是真实的，但是我查到了2004年曾有这样一则新闻：

2月2日：索格斯的琳达·雷伯恩（44岁）和迈克尔·贝里（23岁）被双双谋杀于家中。根据警方的说法，雷伯恩的丈夫戴维·雷伯恩（David Rayburn）用一把榔头杀害了他的妻子和继子。两名死者的尸体在两间相邻的卧室中被发现。而戴维·雷伯恩留下一封遗书后，走进了地下室，然后上吊身亡。

以下就是这段凶手留下的密码：

（图片已删除）

密码的前两行被圈出的长方形并不是凶手画的，这是他们的一位家庭成员在事后画上去的。

假设以上所有事情都是真实的，那么这就是现实世界中的一段尚未被破解的密码。没有人知道这段信息究竟是什么，甚至没有人知道这究竟是不是一段信息。

如果任何人能够破译出这段密码，请联系我。

发表于2006年1月30日上午10：15·411条评论

密码学家通常都非常具有怀疑精神，有些人甚至会说密码学家简直都有妄想症。因此，雷巴和施奈尔都对这段密码的真实性提出了质疑。但是，从施奈尔找到的这段新闻报道中，我们至少可以确定这件双重谋杀及自杀事件确实是一起真实事件。2015年8月，我曾致电罗纳德·焦尔杰蒂（Ronald Giorgetti）警官询问此事。焦尔杰蒂警官在案发后勘察过该案的犯罪现场，但他并没有在现场看到任何与上述密码类似的东西。然而，考虑到该案的犯罪现场相当可怕，也许焦尔杰蒂警官并不一定能注意到现场的所有物件。警官建议我联系另一个部门——地方检察官办公室，他认为我从那里也许能获取更多信息。在我写作本书时，我提交给地方检察官办公室的申请仍然未获得批准。

报纸上的新闻称，警方完全搞不清雷伯恩谋杀妻儿的动机是什么［根据《波士顿先驱报》（*The Boston Herald*）的说法，凶器是一把需要用双手抡打的长柄大铁锤］，也搞不清雷伯恩为什么要自杀。雷伯恩似乎并没有精神方面的疾病，也没有人见过他与家人发生争执。事实上，在谋杀发生前24小时，雷伯恩还组织了一个聚会，和朋友一起收看超级碗比赛。警方在案发现场的厨房桌子上确实发现了一封遗书，但是雷伯恩在这封遗书中既没有讲述谋杀的动机，也没有解释自己的行为。《波士顿先驱报》引用了一名知情人的说法，据此人描述，这封遗书“非常简短，基本上凶手只说了他很抱歉，以及一些其他的事情，但却完全没有解释他为什么要这么做。”[注]

一些证据显示，这家人似乎有一些经济上的困难。在谋杀发生前不到一个月，琳达曾经填写过一份城镇调查表格。在这份调查表格中，琳

达填写的她丈夫的职业是“互联网技术人员”，然而事实上她的丈夫当时并没有工作。[注]根据《波士顿先驱报》的说法，由于经济上的困难，雷伯恩差点儿被从他的房子里赶出去。然而，索格斯的警察局局长詹姆斯·J.麦凯（James J.Mackey）表示，雷伯恩的这封自杀遗书中并没有提到任何经济上的困难。

那么，凶手留下的这段密码中是否包含某些在自杀遗书中没有提到的信息呢？在施奈尔的这条博文发布以后的多年间，博客的读者们一共留下了411条留言。这些留言主要讨论的都是这则密码的破译问题，但也有一些留言讨论了这起案件的其他方面。

一位网名为“ChrisW”的读者最先提出了一条非常重要的观点。ChrisW写道：“我不知道这是不是一个恶作剧，但是我注意到，在这段密码中，只有小写字母被横线拦腰截断，并且非字母的字符仅出现在密码的两侧。”[注]

也许，写下这些字符的人（应该是凶手雷伯恩，但没有人知道究竟是不是他）不希望将像C和c这样的大小写字母被混淆。为了区分大小写字母而在每一个小写字母上面都画一条下划线似乎也没有必要，但这种做法确实能清楚地表明整段密码中字母的大小写。如果这些字符的大小写是一个必须表示清楚的重要信息，那么这段密码就有可能是一段口令[注]。以上结论是由一位名叫“Davi Ottenheimer”的网友在留言中提到的，但是这位网友仅仅提出了这个结论，而没有给出论据。[注]

在破解密码的过程中，密码的上下文信息很可能会给出一些重要的线索。根据这种思路，另一位网友“Cher”引用了施奈尔收到的原始电子邮件中的一句话（“他死后留下了一些令人不安的物件”）。这位网友评论道：“如果能够知道这些令人不安的物件究竟是什么，也许我们就能破译出这段密码。”[注]

针对Cher的这条留言，另一位网友发表了一段很长的回复。接下来我把这位网友的回复全文复制如下：

肯（Ken）·2006年2月2日上午8：17

你好——

我就是把这段密码以电子邮件的方式发给布鲁斯的人。感谢布鲁斯贴出了这段密码。

下面我来回答一些最常见的问题。这段密码是在一个打开的公文包里发现的，这个公文包就放在凶手上吊的地点旁边。在这个公文包里有一些儿童色情光盘，并且还有一些全新的性爱用品，比如带有天鹅绒的手铐。

自杀遗书是在厨房的桌子上被发现的。这封遗书写道：“原谅我，我必须这样做。”其他几位家庭成员的名字是：帕特（Pat）、珍（Jenn）、克里斯滕（Kristen），以及帕特的丈夫查理（Charlie）。

珍、克里斯滕和迈克尔的姓都是贝里（Berry），而不是雷伯恩（Rayburn）。他们家还有两只猫，名字分别是奥齐（Ozzie）和卢克（Luke）。

这（段密码）是一份复印件。他们家的一些朋友曾试图破译这份密码，并在这张纸上留下了一些痕迹，我把这些痕迹都涂白了，因为我不希望这些笔迹让看到密码的人感到迷惑。此外，这张纸上的折痕也是我留下的。许多年前，凶手雷伯恩就被诊断患有双向情感障碍。然而不管是雷伯恩本人还是他的父母，都从来没有把这一事实告诉我的朋友琳达。雷伯恩是一个技术发烧友，他喜欢《星球大战》和音乐。警方并没有针对这起谋杀进行过深入的调查，因为在他们看来……这“既是一起尚未侦破的案子，又是一起已经侦破的案子”。警方已经找到了凶手和凶器，我理解有些网友认为我发这段密码是为了搞恶作剧。事实不是这样的。我只是希望也许某个人能够认出这个密码，然后说：“我以前看过这种类型的密码。”有的网友说这段密码可能是一段口令，这也许是合理的。因为在发现这段密码的公文包附近还放着一台笔记本电脑。正如我所说的那样，警方并没有对这起案件进行过深入的调查。他们甚至不

能（或者不愿意）把对两名死者死亡时间的推断精确到小于24小时的范围内。

我只把这段密码发给了布鲁斯一个人。最近我在我的抽屉里看到了这段密码，并决定做些什么。我感谢每个人在这件事上花费的时间和精力。

谢谢你，

肯

我问布鲁斯，发表这条留言的人是否真的是通过电子邮件将这段密码发送出来的，并且问布鲁斯能不能让我和这个人联系。然而布鲁斯的回复是："不，我不能。因为我完全不知道他是谁。"[注]此外，我还询问布鲁斯，除了他发表在博客上的内容以外，他是否还对这起案件有其他了解。对于我的这个问题，布鲁斯也给出了否定的回答。

罗纳德·焦尔杰蒂警官告诉我，他并没有在案发现场看到过任何儿童色情光盘或者手铐。但是，他也没有明确地说这些东西绝对不存在，他只是再次建议我联系地方检察官办公室获取更确切的信息。

在网友肯发表上述留言以后，情况变得糟糕起来。肯声称他只是想帮助死者家属，他的这番说辞听起来也很真诚。然而，当珍发现了这段博文以后，肯和珍的友谊也破裂了。导致这场决裂的主要问题是，在这篇博文下面出现了一些讨厌的回复（当然，任何回复率高的博文下面几乎都有这种恶意的留言）。除此之外，网友还在某些留言中攻击了其中一名死者。于是接下来两拨人为此发生了争执，其中一拨人声称他们是死者的朋友或亲属（我个人认为他们确实是死者的朋友或亲属），而另一拨人则声称他们是凶手的朋友或亲属。对于这些争执的细节我就不复述了，以下我只引用一名试图帮助大家破译密码的网友的留言。

网友"Ganzfeld"认为，这段所谓的"密码"其实只是一些文件或目录名称的清单，而纵列则是访问这些内容所需要的口令。他写道：

> 这种目录名称的风格非常像“用户数据”目录所使用的（8个字母的）随机目录名称。在这段所谓的“密码”中，没有任何一行超过8个字符，这一点也能够支持我的上述结论。这段“密码”中的大部分横行中都包含7个或者8个字符，我觉得这不太可能是一种巧合。这说明这些内容是某种文件系统的一部分……这并不是一些加密的文字。
>
> 我认为有3个或者5个字符的几行是目录，有7个或者8个字符的几行是上述目录对应的子目录，或者是这些目录下的文件名。
>
> 因此这张纸上写的所有内容其实是某处的一个服务器上的目录列表，以及访问这些目录所需要的口令。[注]

在发表上述留言以后的第二天早上，网友“Ganzfeld”再次留言否定了整页内容都是口令的说法。网友“Ganzfeld”特别指出，“Mmg”这一行作为口令来说实在说不通。对这张纸上的内容的另外一个方面，网友“Ganzfeld”也提出了一种可能的解释。

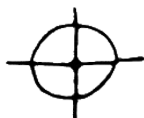
> 此外，在那些“潦草”的字母中也有一条重要线索。我认为在字母“k”下面的字母实际上是“L”……因为这个字母和另外一个字母“L”的写法类似——向下的一笔都拖得过长。因此，那几个潦草的字母应该是L、M和H。我个人认为这三个字母的意思是低（Low）、中（Medium）和高（High）。这几个字指的可能是文件的分辨率。[注]

也许，我们永远无法知道凶手留下的这段“密码”究竟是文件目录、口令，还是一段加密的信息。但是，如果当地的地方检察官办公室能够回复我的申请的话，我想我们至少可以搞清楚这段密码究竟是真实存在的，还是别人伪造的。

接下来我要向读者介绍另一起凶案，这起案件很像是雷伯恩案的一

个加长版本。

苏珊案



你知道，每个人都会使用“结束”这个词，甚至会用这个词来开玩笑。……然而对我来说，事情永远没有办法“结束”。并且我相信，对于大部分孩子被谋杀的父母，或者孩子不幸在凶案中受伤害的父母而言，事情也永远没有办法“结束”。因为从事情发生的那天起，你的生活已经被永远地改变了。

——约翰·沃尔什[注]

和前文提到的贝齐·韦尔斯一样，苏珊·考克斯（Susan Cox）也是一位因为嫁错了人而被杀害的无辜女性。2001年4月，她与乔希·鲍威尔（Josh Powell）结婚，婚后改名为苏珊·鲍威尔。婚后，苏珊遇到的第一桩麻烦来自她丈夫的家人。乔希的兄弟约翰尼（Johnny）有精神病史，然而给苏珊带来更大麻烦的是乔希的爸爸史蒂夫（Steve）。史蒂夫希望儿媳苏珊不仅做乔希的妻子，还要做他自己的妻子。乔希和苏珊夫妇二人因此搬出了史蒂夫在华盛顿州的房子，去犹他州居住。由于乔希和苏珊夫妇二人的经济状况不好，此前史蒂夫的房子算是给他们提供了一个容身之处。在儿子和儿媳搬走以后，史蒂夫似乎仍然不肯接受事实，他继续骚扰儿媳，给苏珊寄去了自己的裸照。

史蒂夫对苏珊的迷恋似乎已经成为一种执念，他不仅创作了几十首关于苏珊的情歌，还在整整17本螺旋笔记本中写满了关于苏珊的内容，

总共超过2 330页。虽然苏珊似乎并不知道下列情况，但是当她还住在史蒂夫的房子里时，史蒂夫偷拍了数百张苏珊的照片，照片中的苏珊做什么事情的都有：比如吃麦片、使用卫生棉条等。

苏珊以为，搬到犹他州以后，情况就会好起来，然而事情的发展并没有如她所愿。在她和丈夫乔希添了两个儿子以后，乔希的性格变了。他不仅变成一个控制欲极强的人，而且在经济上也成了苏珊的负担。

苏珊于2009年12月7日失踪，当时有大量的间接证据显示凶手可能是她的丈夫乔希。在苏珊失踪仅仅48小时以后，乔希租了一辆汽车，并在两天内驾着这辆车行驶了807英里。乔希从未解释过自己在这两天中干了什么。乔希的父亲史蒂夫在这两天中请假未去上班，他也同样不能解释这两天中自己去了哪里。苏珊的父亲以及警方都怀疑乔希和史蒂夫在这两天中将苏珊的尸体移到了别处。警方将乔希列为犯罪嫌疑人，并且将乔希描述为一个“极度不合作”[注]的嫌疑人。

也许警方曾经想过，他们可以继续收集证据，并且最终用充分的证据起诉乔希以及她的一名或多名家庭成员，但他们的这个想法显然落了空。此案后来变成美国历史上最大的失踪人口调查事件，苏珊的尸体从未被找到，也没有任何人以谋杀苏珊的罪名（或者其他较轻的罪名）被起诉。

2011年9月22日，警方终于以其他罪名将史蒂夫逮捕。史蒂夫因持有儿童色情内容以及14项偷窥罪名而被捕。然而在这14项偷窥罪名中，史蒂夫偷窥的对象并不是苏珊，而是他邻居的两个女儿，这两名女孩当时分别是8岁和9岁。警方的最终调查结论是：史蒂夫·鲍威尔与苏珊的失踪并无直接联系，但他可能在苏珊失踪以后获知了案件的某些细节。

警方还发现，乔希喜欢看卡通色情片。虽然在这些卡通色情片中，也有许多影片涉及未成年人，但这处于一个法律的灰色地带，因为这些色情片中并没有出现真人。

苏珊的父母查克·考克斯（Chuck Cox）和朱迪·考克斯（Judy Cox）

都相信，乔希应该为他们女儿的失踪负责。他们为争夺两名外孙的抚养权而对簿公堂。由于史蒂夫住处的环境极不适合儿童生活，而乔希不仅拥有一些奇怪的色情片，还是苏珊失踪事件的嫌疑人，所以查克和朱迪夫妇最终胜诉，赢得了两名外孙的抚养权。

后来，当乔希和苏珊的两个儿子分别长到5岁和7岁时，法庭还只允许乔希在有人监控的情况下探访这两名儿童。2012年2月5日，两个孩子去乔希家拜访父亲，乔希开门让他们进屋以后，随后立即关上门并上了锁，不允许其他人员进入。此前，乔希已经在屋子周围洒上了汽油。两个孩子进屋以后，乔希点燃了地上的汽油。他的房屋随后爆炸。

事后，警方的调查人员发现，乔希的两个儿子的死因都是吸入过量烟雾。然而，这两名儿童的头骨都部分缺失，警方相信这是因为他们曾被人用一把短柄斧头攻击过。此外，警方还发现，乔希早就计划进行这次谋杀，在案发前一天，他已将儿子的玩具送给了别人。

在此案发生大约一年多后，2013年2月11日，乔希的兄弟迈克自杀身亡。此前，警方的调查重点就已经开始转向迈克是否曾经参与谋杀或者谋杀后的掩饰工作。在迈克死后，警方才向公众透露，他们认为迈克“深度参与”了移走苏珊尸体的过程。[注]

苏珊失踪后仅仅几个星期，迈克在俄勒冈州的一处垃圾场中丢弃过一辆汽车。一位侦探偶然间发现了这件事。当迈克致电一家位于科罗拉多州博尔德市的成像公司要求购买一幅垃圾场的高清卫星照片时，这位侦探恰巧在这家成像公司中。迈克购买这幅照片是为了看看自己丢在那里的车辆是否已经被粉碎并出售。得知这一消息后，警方迅速赶往垃圾场找到了迈克丢弃的汽车。警犬在这辆车中闻到了尸体腐烂的气味。

除此之外，警方还发现了另一条证明迈克曾经帮助乔希抛尸的间接证据：在乔希自杀前大约两个月，他曾联系自己的人寿保险公司修改了保险的受益人。乔希的人寿保险赔偿金共有2 500 000美元，他将赔偿金中的93%留给了迈克。

在上述几起死亡事件发生之前，警方已经监听了鲍威尔家所有家庭成员的电话。但是乔希和迈克都不信任电话，也不用这种通信方式进行交流。这也不要紧，警方还在2011年8月至2011年10月期间监控了乔希和迈克的电脑。不幸的是，乔希和迈克居然在电脑上使用了一套加密系统，不管是警方、美国联邦调查局，还是软件制造商都无法破解这套加密系统。

警方从未向公众透露乔希和迈克使用的究竟是何种加密系统。现实世界中存在许多这种未被破译的密码。我个人认为，在这些案件中最令人失望的一点是，美国国家安全局事实上很可能完全有能力破解其中的大部分密码。然而，即便美国国家安全局真的有这样的能力，他们仍有充分的理由拒绝破译这些密码。为了理解这些理由，让我们来考虑以下这两种情形：

1. 一帮恐怖分子正在计划进行一次规模和“9·11”恐怖袭击事件相当的袭击。为了保持操作上的安全性，这帮恐怖分子决定使用密码。他们挑选了一种他们认为美国国家安全局无法破译的加密系统。然而，他们不可能完全确定美国国家安全局没有能力破译这些密码，因为美国国家安全局一直将自己的许多能力和技术对公众保密。因此，恐怖分子选择了错误的加密系统，美国国家安全局成功地破译了恐怖分子的密码，并借此获取了重要的情报。在这些情报的帮助下，美国情报机构采取行动，防止了这次大规模恐怖袭击的发生。

2. 一帮恐怖分子正在计划进行一次规模和“9·11”恐怖袭击事件相当的袭击。为了保持操作上的安全性，这帮恐怖分子决定使用密码。此前，这个恐怖组织一直密切关注许多美国法庭的庭审案件，在这些案件中，美国国家安全局的工作人员以证人的身份，讲述了多种密码破译结果的精确性。在范围极广的许多罪案的庭审中，美国国家安全局的这些证词帮助检方人员成功将罪犯定罪。然而，通过关注这些庭审案例，恐怖分子发现，某一种特定的加密系统似乎从未在法庭上被提起过。于是，恐怖组织据此猜想，美国国

> 家安全局无法破译这种加密系统产生的密码，于是选择使用了这种加密系统。情报机构虽然截获了恐怖分子之间的一些通信内容，却没有办法破译他们使用的密码。最终，美国情报机构未能收到关于这次恐怖袭击的提前警告。恐怖分子成功实施了袭击，数千人因此丧生。

我相信，每一个在执法和情报机构工作的人都希望鲍威尔案能够取得令人满意的侦破结果。然而，如果情报机构帮助执法机构破译那些加密的电子邮件，并把这些破译后的邮件当作庭审证据的话，可能会在其他方面产生负面的影响。

此后，鲍威尔案还出现了一个意想不到的转折。史蒂夫·鲍威尔偷窥罪行的两名受害者买下了史蒂夫的房子，并且允许苏珊的家人进入房子内部进行搜查。这次搜查似乎取得了一些可能有帮助的线索，媒体对这一事件进行了以下报道：

> 考克斯一家告诉《赫芬顿邮报》（HuffPost），他们发现了若干可能与案件有关的物品，其中包括一个装有计算机编码文件的盒子。考克斯一家表示，他们希望这些文件包含某种信息，能帮助联邦调查局破译乔希·鲍威尔电脑中的文件。乔希·鲍威尔生前拥有一部高度加密的电脑，警方一直无法破解该电脑上的加密系统，因此也就未能获取电脑中的内容。[注]

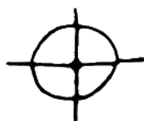
然而，这篇报道并没有解释所谓的“计算机编码文件”究竟是指什么。

在最近的几十年中，不仅密码分析技术有了长足的发展，计算机的计算能力也获得了巨大的提高，并且这种高速发展的趋势在未来还会继续保持。如果警方还保存着鲍威尔案中的电子邮件和电脑硬盘的话，那么即使没有政府机构的帮助，我们仍有希望看到这些内容在未来的某个

时刻被成功破译。当然，我相信对于苏珊的父母而言，无论案情的侦破取得怎样的进展，都不会使他们完全解脱。然而，如果破译工作能够取得成功的话，也许至少可以解开一个谜题，那就是：在苏珊身上究竟发生过什么。也许警方能最终找到苏珊的遗体，让苏珊的父母好好地埋葬枉死多年的女儿。

在鲍威尔案中，警方需要破译的内容主要是经过加密的电子邮件。然而在许多其他案件中，需要破解的是电脑硬盘。这种情况会给警方带来许多麻烦。接下来，我会介绍一起发生在德国的案件。从这个案件中，我们就可以看出破解加密硬盘有多么难。

德国的蒙面男子



1992年，德国警方通缉了一名男子，这名男子的外形素描图如图5–8所示。这名男子在夜晚穿着如图所示的伪装服饰，在校园及青少年中心性侵儿童。媒体将这名通缉犯称为“蒙面男子”或者“黑衣男子”。1994年，这名蒙面男子开始非法侵入住宅寻找受害者。



图5-8 蒙面男人的外形素描图

除了性侵和非法侵入住宅以外，这名蒙面男子还制造了多起谋杀案。警方发现，这名蒙面男子的作案规律是每3年杀死一个人。他的第一名受害者是1992年被杀的13岁少年斯特凡·雅尔（Stefan Jahr）。1995年，8岁的丹尼斯·罗斯特尔（Dennis Rostel）在德国被这名蒙面男子诱拐，他的尸体最后在丹麦被发现。接下来的一起符合蒙面男子犯案特征的谋杀发生于荷兰，受害者是11岁的尼基·费斯塔彭（Nicky Verstappen）。2001年，蒙面男子又谋杀了9岁的丹尼斯·克莱因（Dennis Klein），他在德国被诱拐，尸体也在德国被发现。而下一位受害者——11岁的乔纳森·库隆（Jonathan Coulom）在法国失踪，尸体也在法国被发现。

因为本案具有跨国性质，德国、荷兰、法国的相关部门展开了密切的合作。此案也吸引了媒体的高度关注。

最终，一名1995年被蒙面男子性侵的受害者向警方提供了一条重要线索。根据这条线索，警方于2011年4月逮捕了马丁·奈伊（Martin Ney）。经过第一轮审讯，奈伊承认了在德国犯下的3起谋杀，以及约40宗性侵儿童的罪行。但是奈伊不承认自己杀害了尼基·费斯塔彭和乔纳森·库隆，也没有证据能证明他确实是这两起凶案的凶手。但奈伊仍是上述两宗凶案的嫌疑人。

奈伊因他承认犯下的三起谋杀被判终身监禁，目前他正在德国的一处监狱中服刑。不管警方能否最终确认奈伊是其他几宗谋杀的凶手，他的生活都不会再发生改变了。但是对于那几起凶案的受害者亲属而言，找到这些案件的真凶却仍然非常重要。此外，找到这几起谋杀案的真凶还能帮助人们最终确认谋杀尼基·费斯塔彭和乔纳森·库隆的凶手是否还在逍遥法外，继续危害社会治安。如果奈伊确实不是上述几起凶案的凶手，那么警方就必须找到犯下这几起凶案的真凶，才能消除此人对社会的威胁。那么，善于破译密码的人能否帮助警方找到问题的答案呢？答案也许是肯定的，而且，破译人员解开与该案有关的密码、帮警方找出

真凶的概率还在不断升高。

在奈伊被捕以后，警方没收了他的电脑，并发现该电脑配有一个加密的硬盘。在奈伊位于汉堡的公寓中，还藏有另外一些存储设备。警方初次搜查的时候并没有发现这些设备，因为它们被非常精心地隐藏了起来。几个月以后，奈伊的公寓被租给了一位新租户，这位新租户发现了这些被奈伊藏起来的存储设备，并交给了警方。如果警方能够读取这些存储设备中的内容，也许更多相关的案件就能告破。然而，这些存储设备所用的加密系统相当强大，并且奈伊拒绝向警方提供相关的口令。

德国的密码破译专家克劳斯·施梅建议警方把这些加密的内容公布在网络上，这样世界各地的密码破译者就都可以尝试来破译这些内容了。然而，我认为警方恐怕不会采纳这样的建议。因为这些加密文件中可能包含淫秽的内容，如果某位成功破译了这些内容的人不负责任地传播这些内容，就会使罪案的受害者受到进一步的伤害。基于这样的原因，警方肯定不能将这些加密内容公之于众。

然而，施梅建议采取的这种方法还是有希望以另一种方式实现的。施梅指出：

> 警方并没有必要公布密文的一部分。文件加密程序通常会检验用于解密的密钥是否正确（用错误的密钥来破译密文只会得到毫无意义的信息）。为了实现此功能，程序通常会用密钥来检验一些预先加密过的无意义的非秘密信息，这就可以达到判断密钥是否正确的目的。警方只要将这些非秘密的信息（包括明文以及加密后的密文）公之于众，就可以在不泄露任何实际数据的情况下，让每个人都尝试去破译这个加密系统。(注)

然而，警方不仅拒绝让更多拥有密码破译技能的人参与破译的工作，甚至也拒绝透露奈伊使用的究竟是何种加密模式。目前，在市场上存在大量不同的加密产品，警方选择不向公众透露究竟是哪种加密产品

也是明智的。但是，密码分析的技术一直在稳步提高，计算机的运算速度也正在变得越来越快。也许就在今年的晚些时候，或者明年，奈伊所使用的加密系统就有可能被成功破译。虽然只有时间才能告诉我们真正的答案，但是，由于奈伊目前只有40多岁，我充分相信他会活着看到自己的密码被破译的那一天。

也许，阅读本书的读者中会有某位密码破译方面的专家能够对本案做出一些贡献。因此，我将关于本案的一段话复制如下，这其中包含一些案件的细节，还包括负责该案的具体警方部门，有线索的读者可以尝试与该部门联系。

> 马丁·奈伊的电脑和硬盘目前被存放在下萨克森州警察局的司法科学研究所里。该所有多名信息技术司法科学方面的专家。根据凯·托马斯·布雷阿斯（Kai Thomas Breas）的说法，警方还咨询过两名计算机科学方面的教授。在他们的帮助下，解码软件的破解速度有望从每秒90个密码提高到每秒125 000个密码。[注]

虽然许多其他案件中也包含尚未被破解的加密电子邮件或加密硬盘，但是在本书中我不打算继续向读者介绍这些案件。我这么做的原因之一是：这类加密信息很难复制在书本中，因此我无法向希望自行尝试破解这些未解之谜的读者提供相关的资料。虽然这些信息可以公布在本书的官方网站上，但是由于我在前文中已经提到的原因，执法部门很可能并不希望这些内容被公之于众。

如果你真的希望帮助警方打击犯罪，请尽量多学习数学和计算机科学方面的知识，并加入执法队伍，或是可以为执法机构做外包工作的其他机构！

---

1. Cheri L.Farnsworth, Adirondack Enigma: The Depraved Intellect and Mysterious Life of North Country Wife Killer Henry Debosnys (Charleston, SC: The History Press, 2010).

2. Farnsworth, Adirondack Enigma, p. 26, quoting a reporter who visited Henry in jail.
3. Farnsworth, Adirondack Enigma, 69.
4. Farnsworth, Adirondack Enigma, 27.
5. Farnsworth, Adirondack Enigma, 69.
6. Farnsworth, Adirondack Enigma, 69–71.
7. Farnsworth, Adirondack Enigma, 71–72.
8. Farnsworth, Adirondack Enigma, 72.
9. Farnsworth, Adirondack Enigma, 72.
10. Farnsworth, Adirondack Enigma, 72.
11. Farnsworth, Adirondack Enigma, 72–73.
12. Farnsworth, Adirondack Enigma, 73.
13. Farnsworth, Adirondack Enigma, 73.
14. Farnsworth, Adirondack Enigma, 73.
15. Farnsworth, Adirondack Enigma, 73.
16. Farnsworth, Adirondack Enigma, 43.
17. Farnsworth, Adirondack Enigma, 76.
18. Farnsworth, Adirondack Enigma, 76.
19. Farnsworth, Adirondack Enigma, 77–78.
20. Farnsworth, Adirondack Enigma, 79–80.
21. Farnsworth, Adirondack Enigma, 80.
22. Farnsworth, Adirondack Enigma, 80–81.
23. Philadelphia Times, August 11, 1882.
24. Farnsworth, Adirondack Enigma, 27 and 63.
25. See http://www.isi.edu/~knight/ to get an idea of the lively, creative, eccentric way he views the world.
26. E-mail received by the author on May 8, 2015.
27. “mason”既指共济会，也指石匠，共济会成员也自称石匠。——译者注
28. Farnsworth, Adirondack Enigma, 107.
29. American Cryptogram Association, http://cryptogram.org/.

30. Taken from Tom Mahon and James J.Gillogly, Decoding the IRA (Cork, Ireland: Mercier Press, 2008), 266, fig. 27, pt. 9.

31. Tom Mahon and James J.Gillogly, Decoding the IRA (Cork, Ireland: Mercier Press, 2008), 48.

32. Mahon and Gillogly, 33.

33. Mahon and Gillogly, 53.

34. Brainy Quotes, John Walsh quotes, http://www.brainyquote.com/quotes/authors/j/john_walsh.html.

35. America’s Most Wanted, http://en.wikipedia.org/wiki/America's_Most_Wanted#Profiling_missing _persons. The man was captured in April 2008.

36. That would give us 156 distinct symbols instead of the 155 we actually observed. That’s why I used the word “approximately.”

37. Nick Pelling, Cipher Mysteries blog, http://www.ciphermysteries.com/2014/05/19/cracking-the-scorpion-ciphers.

38. “大学炸弹客”（the Unabomber）在1978—1995年间引发了10余场爆炸事件，导致3人死亡，23人受伤。他因喜欢在大学里和航班上放置炸弹而得名。——编者注

39. Successories website, John Walsh Quotes, http://www.successories.com/iquote/author/6223/john-walsh-quotes/1.

40. IMDb, America’s Most Wanted, http://www.imdb.com/title/tt0094415/quotes.

41. “菲尼克斯”（Phoenix）与“腓尼基人”（Phoenician）词根相似，或许这就是该杂志得名由来。——编者注

42. It was actually February 2, 2004. The bodies were found on the third.

43. Tom Farmer, “Suicide Note Leaves Motive for Saugus Killings a Mystery,” The Boston Herald, February 5, 2004, p. 14.

44. Mac Daniel and Diane Allen, “Killings, Suicide Baffle Authorities. Husband Left Note; Motive a Mystery,” The Boston Globe, February 5, 2004, 3rd ed., p. B1.

45. Posted January 30, 2006, 11:16 a.m.

46. 我们把平时登录网站、电子邮箱或银行取款时输入的需要保密的数字或字符也叫“密码”，它又叫“口令”，和本书主要讨论的“密码”含义不同。——编者注

47. Posted January 30, 2006, 11:42 a.m.

48. Posted January 31, 2006, 11:58 a.m.

49. E-mail received by the author on August 3, 2015.

50. Posted February 18, 2006, 1:29 p.m.

51. Posted February 19, 2006, 7:02 a.m.

52. Successories, John Walsh Quotes, http://www.successories.com/iquote/author/6223/john - walsh-quotes/8.

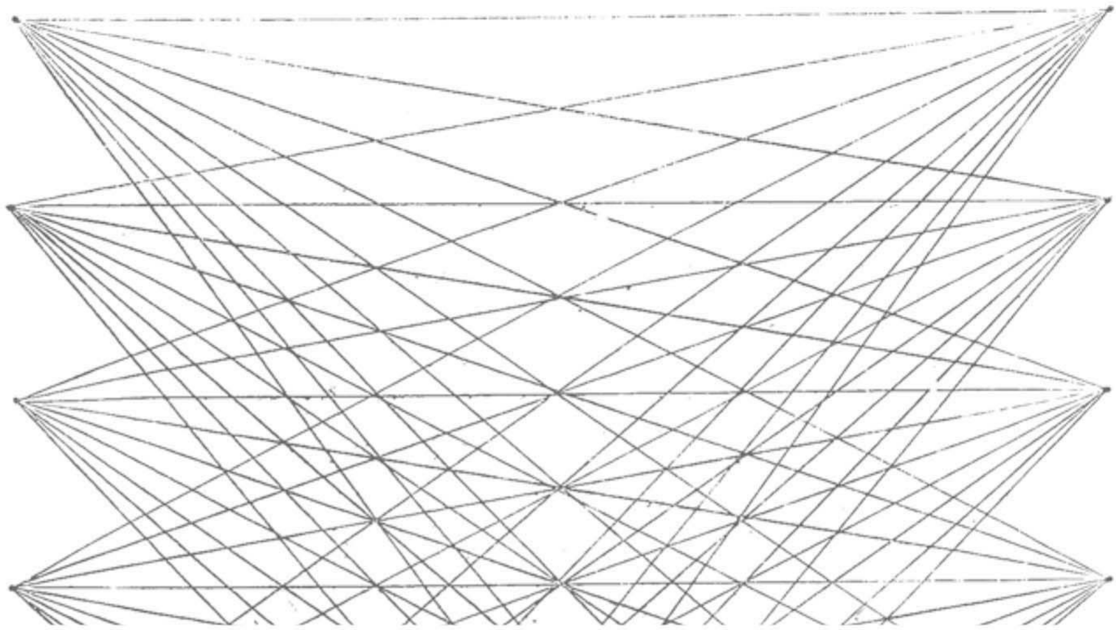
53. Greg Olsen and Rebecca Morris, If I Can’t Have You: Susan Powell, Her Mysterious Disappear-ance, and the Murder of Her Children (New York: St. Martin’s Press, 2014), 102. Also see p. 228.

54. Anonymous, “Police Close Susan Powell Case, Offer New Details,” USA Today, May 20, 2013, available online at http://www.usatoday.com/story/news/nation/2013/05/20/susan-powell - case/2344681/.

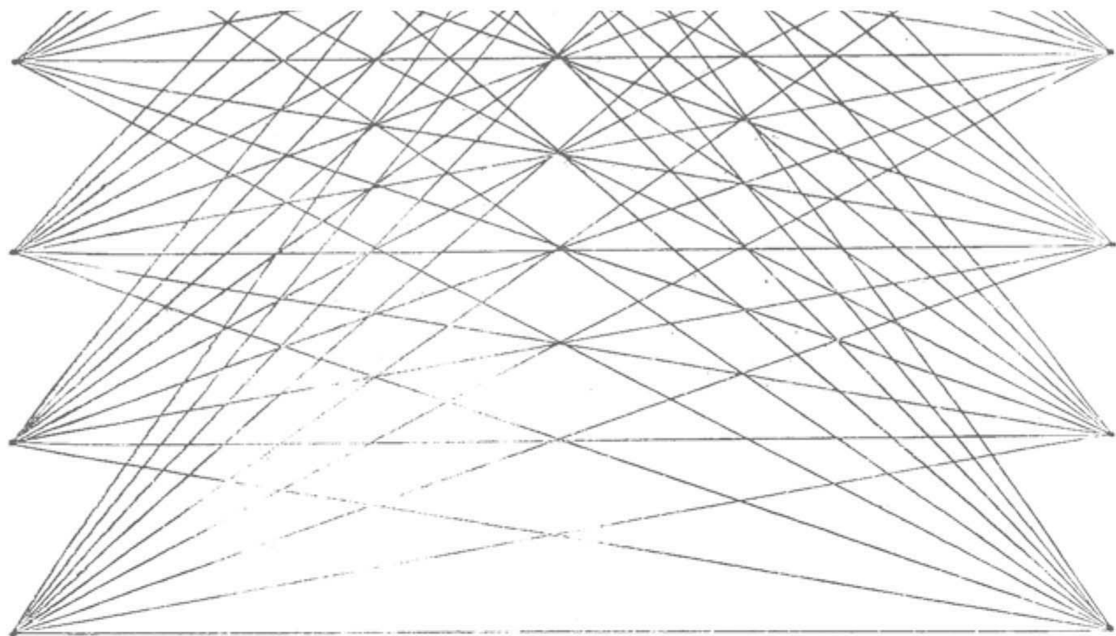
55. David Lohr, “Susan Powell’s Parents Search For Clues in Father-in-Law’s Former Home,” Huff-ington Post, May 27, 2014, available online at http://www.huffingtonpost.com/2014/05/27 /susan-powell-missing-clues_n_5398147.html.

56. Communication with the author.

57. Ingo Wagner, “Verschlüsselt und nicht knackbar, Polizei scheitert an Festplatten des ‘Masken manns,’ ” Focus Magazine, January 23, 2012. Available online at http://www.focus.de/panorama /welt/verschluesselt-und-nicht-knackbar-polizei-scheitert-an-festplatten-des-maskenmanns _aid_705621.html. Quoted portion translated by the author.

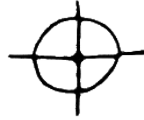


第6章
受害者密码



在上一章中，我向读者介绍了一些与谋杀案凶手相关的尚未被破解的密码，然而，在各种死亡事件中，还存在其他种类的密码。有时，谋杀案的受害者也会在死前留下密码。如果解开这些密码，我们是否就能找出凶手的身份呢？在安东尼·鲍彻（Anthony Boucher）的短篇小说《QL696.C9》(注)中，他就构思出了这样一个故事。在这篇小说中，一名图书馆管理员坐在打字机前被枪杀。在生命的最后时刻，受害者在打字机上留下了一些奇怪的文字："QL696.C9"——小说的题目正是来自这段奇怪的文字。这段奇怪的遗言看起来像是死者供职的国会图书馆图书卡上的图书目录号码。如果死者生前在打字纸上敲出"杀死我的凶手是……"这样的字句，那么凶手就会在离开前销毁打字机上的这张纸。然而，由于死者被杀前正在打一份待购书籍的清单，因此凶手可能只会认为死者临死前还在清单上添上一条目录号的行为很有意思，便没有销毁打字机上的这张纸。死者是否真的如此沉迷工作，以至于要拼尽生前最后的力气去完成一项工作任务呢？在这篇小说中，随着调查的进行，侦探将嫌疑人的范围缩小到了以下几个人之间：低级图书馆管理员斯特拉·斯威夫特（Stella Swift），儿童图书馆管理员科拉·贾维斯（Cora Jarvis），图书馆赞助人詹姆斯·斯蒂克尼（James Stickney），以及高中老师诺伯特·乌特（Norbert Utter）。然而，事实上侦探手中唯一的线索只有死者生前留下的这条奇怪的信息而已。你能够根据这条线索判断出谁是真正的凶手吗？这个问题的答案将在本章的结尾处揭晓。而下文中，我将向读者介绍三起发生在现实世界中的谋杀案。虽然即便这三起凶案中的密码被解开，也未必能够直接指出凶手的身份，但是破译出密码背后的信息也许能给警方提供一些有价值的线索，否则这些案子就只能继续作为陈年悬案尘封在档案馆中。也许密码背后的线索能帮助我们最终找到某起悬案背后的真相。

萨默顿男子案



沙滩上的尸体

美国人恐怕很难想象12月1日是一个去沙滩的好日子。然而在澳大利亚，12月1日却是夏季开始的第一天。1948年12月1日清晨，有人在南澳大利亚州阿德莱德的萨默顿沙滩上发现了一名男子的尸体。

警方无法确认这名男子的身份。直到今天，人们仍然称这名男子为“萨默顿男子”。在叙述这个案件时，我会将这名男子称为“萨默顿男子”或者“身份不明的男子”。

死者的年龄看上去约有40多岁，他身体状况良好，肩膀宽阔。警方尤其注意到，死者小腿的肌肉相当发达。据警方推测，这可能是因为死者生前经常穿着高跟骑马靴造成的。当然，还有其他一些可能的原因也会导致小腿肌肉发达，比如死者可能是一名徒步旅行者、击剑者、登山者，或者死者生前经常跳芭蕾舞等。

死者头发的颜色为“金色”，或者“介于金色与红色之间”，或者“红色”，其中还夹杂着一些灰白的头发。对于死者眼睛的颜色也有多种不同的描述，有的说是灰色，有的说是淡褐色。关于淡褐色的眼睛这一点需要进行一些解释：



图6-1 澳大利亚地图，图中标出了阿德莱德及首都堪培拉的地理位置

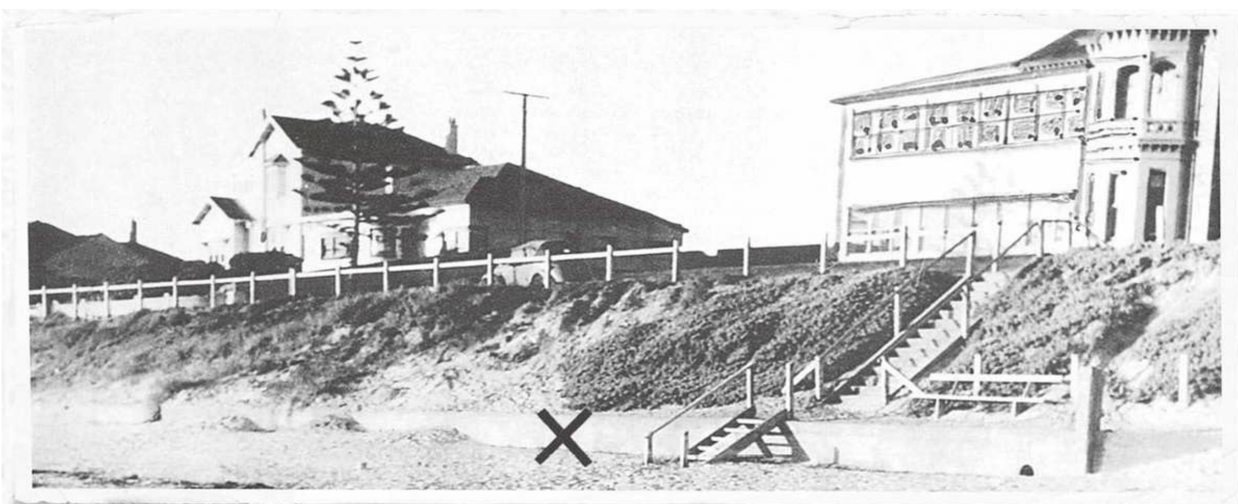


图6-2 在图中画“×”号的地方发现了这名身份不明的男子的尸体

事实上，淡褐色是人们了解最少的眼睛颜色。“淡褐色”的眼睛究竟是什么颜色？这种颜色的眼睛是比较少见的，其实它是其他几种颜色，包括绿色和棕色的组合。淡褐色眼睛所含的黑色素比褐色眼睛所含的黑色素少，但比蓝色眼睛所含的黑色素多。我们很难准确定义淡褐色的眸色，因为所谓淡褐色的眼睛其实可以指多种不同的颜色。淡褐色的眼睛常常会变色，变色的范围在棕色到绿色之间。长着淡褐色眼睛的人虹膜通常会有多种颜色，例如靠近瞳孔的地方是一种颜色，而在外围边缘是另一种颜色。一项研究显示，74%的淡褐色眼睛在瞳孔周围有一个棕色的环状。

目前，人类眼睛的颜色主要被分成4类：褐色、蓝色、绿色和淡褐色。然而，要想更精确地定义眼睛的颜色，4种分类远远不够。
㊟

这位身份不明的男子身高5英尺11英寸（约180厘米），体重约在165~176磅之间（约75~80千克）。他的衣服质量优良。以今天的着装标准来看，死者身上穿着这样的衣服在沙滩上度过一天有点儿太正式了，然而在1948年的时候，穿这样的衣服去沙滩也并不少见。格里·费尔特斯（Gerry Feltus）所著的书的封面就是该男子被发现时的照片，这本书非常全面地介绍了“萨默顿男子”案件的情况。

死者的外套是美国制造的。死者的裤子虽然产自澳大利亚，但是在南澳大利亚是买不到这种裤子的。在20世纪40年代，衣服还是一种比较贵重的东西，因此人们通常会在衣服的标签上写上自己的名字。然而，在死者的衣服上找不到任何标签——他衣服上的标签被人扯掉了。凶手是否不希望警方发现死者的身份呢？死者的鞋子非常合脚，并且最近才打过油，据此判断，死者似乎是一名比较关注自己外表的人。死者脚上所穿的鞋并不是高跟鞋。基本上，从以上的这些信息来看，死者似乎是一个身体状况和经济状况都比较好的人。

死者只有一项不健康的生活习惯，他手上浓重的尼古丁痕迹暗示了这一点。(注)事实上，该男子去世时嘴上还叼着一根香烟。当然，在1948年时，吸烟是一种非常流行的生活习惯，即使是经常运动的人也常常有吸烟的习惯。在1948年时，人们也没有那么重视牙齿的保健，因此，虽然死者缺失了8颗上面的牙齿和8颗下面的牙齿，但这种情况在当时是很常见的，我们也无法从中得到什么额外的线索。在死者缺失的16颗牙齿中，只有两颗在口腔前部，其他都在口腔后部，这种情况在当时也是非常常见的。

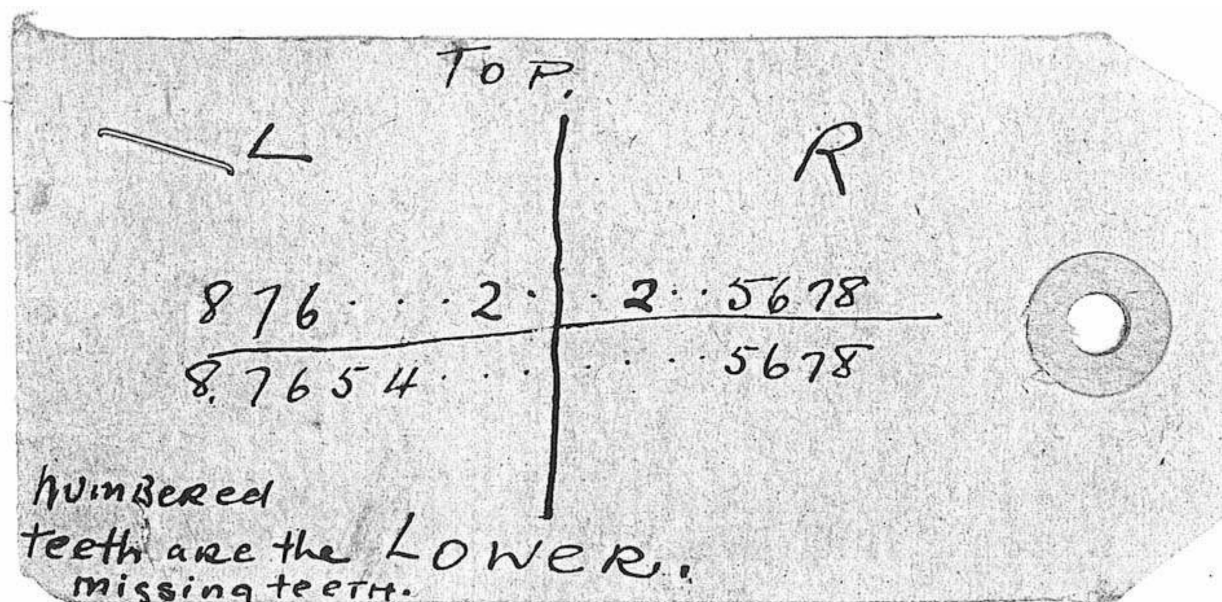


图6-3 这名身份不明的男子的牙齿状况图

虽然死者的尸体是12月1日清晨6：30被发现的，但是后来警方找到了其他的目击证人，他们声称前一晚在沙滩上见过死者。一对已婚夫妇曾在前一天晚上7：00见过这名男子，当时这两名证人还注意到他移动了手臂，因此萨默顿男子在前天晚上7：00应该仍然活着。另一对男女称，他们于前一天晚上8：00在同一地点见过这名身份不明的男子，但是他们没有看到这名男子做出任何动作，因此也就无法判断他当时是否还活着。

在案发10多年以后，即1959年12月5日，又出现了另一位目击证人。这位新证人的证词似乎与此前证人的证词矛盾。新证人向唐奥多尔蒂（Don O'Doherty）警探描述了自己看到的情况，但他不希望透露自己的姓名。唐奥多尔蒂警探对这名证人的证词做了以下汇报：

> 证人称，在萨默顿沙滩上发现尸体的前一天晚上10点左右，他看到有一个人肩上扛着另一个人走在前滩上。证人当时处于单身状态，随行的人有另一名男子和两个女孩。证人已经无法记起随行男子的姓名，但是他提供了两名女孩的名字，那两名女孩是姐妹。证人认为那对姐妹已经搬去别的州了。在目击上述情况时，证人及随行同伴正沿着萨默顿沙滩前往一个邻近的地点，这个邻近的地点被称为"防空洞"。他们看到一个男人肩上扛着另一个人，沿着水边向南走去。证人无法描述那个男人的样子。㊟

为什么这名证人等了10多年的时间才向警方汇报上述情况呢？根据这名证人的说法，他曾与上面提到的那对姐妹讨论过要不要把他们目击到的情况告诉警方，但当时他们都认为，肯定已经有其他人讲过相同的情况了。当目击证人认为有其他证人也看到了相同的情况时，他们的责任感就会下降——不幸的是这种情况确实很常见。然而，这名目击证人的证词产生了一个无法解释的问题：如果死者是前一晚10：00被别人抬到沙滩上，那么为什么其他目击证人会在前一晚的7：00和8：00分别在沙滩上看到死者？当然，我们也可以构想出一些比较复杂的情景让所有

目击证人的证词都成立，但是更加合理的假设是：最后一名目击证人哪里搞错了。毕竟，最后这名目击证人描述的是10多年前的情况。也许证人只是在另一个夜晚看到了他所描述的情况，把一个无关的事件和这名神秘男子的尸体联系在一起。费尔特斯于2003年找到了这名目击证人，并与他进行了交谈。这名证人坚持自己所说的情况准确无误，并加入了一些细节，表明他描述的情况确实发生在萨默顿男子的尸体被发现的前一晚。

在警方的救护车开往医院后，约翰·巴克利·贝内特（John Barkley Bennett）医生对死者进行了快速的尸检。据贝内特医生的估计，死者的死亡时间大约是凌晨2：00，并且贝内特医生认为“死者的样子看上去就像是死于冠状动脉中风”[注]。特别需要指出的是，死者身上并没有发现暴力的痕迹。

如果要追溯过往的暴力事件可能留下的痕迹的话，这名身份不明的男子身上确实有一些伤疤。他的左手腕内侧有3条较短的伤疤，左手肘内侧有一条长约1英寸（2.5厘米）的弯曲疤痕。此外，在上述两处伤疤之间，也就是死者的左前臂上还有一条伤疤，但这条伤疤只有半英寸长，不能排除这只是一处小脓肿留下的痕迹。凯丽·格林伍德（Kerry Greenwook）对死者手腕上的疤痕提出了一种可能的解释：

> 如果一个人穿着油布防水衣，站在盐分很高的海浪里，那么他的非惯用手的袖子就会被打湿，而湿的防水衣会和手腕内侧较薄的皮肤发生刮擦。盐的腐蚀作用很强，在盐分的腐蚀下，防水衣会慢慢在手腕上留下痕迹，然后再发展成伤口和疤痕。在货船上负责协调装卸货物的人需要在非常恶劣的天气中指挥他人装卸货物，因此这类人的手腕上很容易出现死者手腕上的这种伤疤。萨默顿男子很可能是一个惯用右手的人，因为伤疤出现在他的左手手腕上。渔民将这种伤疤称为“鲸鱼痕”。[注]

在货船上从事装卸指挥工作的人手腕上会出现死者手腕上的这类疤痕，而且这类人的手和手指甲通常状况良好，这一点也与死者的情况相符。因为装卸指挥工作是技术活，他们并不需要亲自从事太多体力劳动。

格林伍德的这种解释看起来是有可能成立的，我个人想不出任何反驳的证据。然而，到目前为止，也同样缺乏足够有力的证据来证明格林伍德的推测是正确的。在下文，我还会继续向读者介绍这名死者身上的其他一些奇怪的特征。但现在让我们先来对死者身上穿的衣物做一番更加详细的研究。

由于死者身上穿了不少衣服，警方需要检查的口袋数目也不少。死者口袋中的物件也许能告诉我们更多关于死者的信息。死者随身携带的物件如下：

1条手帕

1张去亨利沙滩的火车票

1张汽车票（票号88708）

1把金属梳子

半盒果汁口香糖

2把梳子

半盒“布莱恩与梅”（Bryant and Mays）牌火柴

香烟［盒子是“陆军俱乐部”（Army Club）牌的，但是里面装着7支“肯西塔斯”（Kensitas）牌的香烟］

1条内裤

1件背心

值得注意的是，死者不仅没有携带任何身份证明，身上也没有任何

钱财。对于这样一个穿着得体的人而言，他的口袋里应该装有现金或者支票本。然而，警方却完全没有发现这些东西，甚至连零钱也找不到。如果这名男子还活着，那么没有身份证明会是一件麻烦的事。没有身份证明就很难找到工作，而且在法律上也会遇到其他麻烦。阿德莱德的警察时常会因为各种原因要求检查路人的身份证件，在当地，有时候警察可能仅仅因为不认识一个人，就拦下这个人要求出示身份证件。

也就是说，在死者随身携带的上述物件中，没有任何物件能够显示死者的身份。另外一个警方未能回答的问题是：这名看起来健康的男子究竟是有意在沙滩上找了这么一个地点自杀，还是被人谋杀的呢？自杀的人有可能会留下遗书，但也有一些自杀者选择不留遗书。据估计，自杀者留下遗书的概率并不高：在不同的人群中，自杀者留下遗书的概率在1/6到50%不等。不管怎么说，如果萨默顿男子是自杀身亡的话，显然他并不认为自己需要留下什么东西来解释自己自杀的原因。

尸体解剖产生的一种理论，以及寻找死者身份的过程

1948年12月2日，约翰·马修·德怀尔（John Matthew Dwyer）对萨默顿男子的尸体进行了解剖。德怀尔此前认为该男子死于毒药，然而他却没能在尸体中发现任何毒药的痕迹。关于毒药检测的细节，只有化学家才能确认。为了进行毒物测试，德怀尔采集了死者的尿液、血液、肝脏组织、肌肉组织以及胃内容物的样本。在后面的死因讨论环节中，我们再来讨论上述测试的结果。

与此同时，为了确认这名死者的身份，警方向媒体公布了尸检后一天拍摄的死者照片。



图6-4 你认识这个人吗？萨默顿男子的正面照和侧面照

在破案的过程中，警方经常会受到假供词的干扰，然而在这起案件中，警方需要克服的却是假身份证明的问题。据报道，共有35人认尸，其中8人都声称自己能够确定地认出死者。然而问题是，这8个人提供了4个完全不同的名字！由于死者拥有“四重身份”的情况不能自圆其说，所以澳大利亚警方扩大了搜索范围。1948年12月21日，警方决定联系所有说英语的国家，广泛寻求关于死者身份的线索，然而这一行动的结果却相当令人失望。虽然澳大利亚警方收到了大量线索，但没有任何一条能帮助警方成功确认死者的身份。到1953年11月为止，各方人士向警方提供的姓名已经多达251个。然而经过调查以后，澳大利亚警方将这251个名字全部排除了。

无人认领的手提箱

警方怀疑，这位身份不明的男子前往沙滩之前，可能将自己的行李

存放在了某处。由于在尸体上并没有发现任何存储行李的票根，所以这完全是一种猜测。1949年1月12日，警方呼吁民众将所有无人认领的行李送往警局，因为这些行李可能是萨默顿男子的行李。虽然寻找萨默顿男子身份的调查陷入了僵局，但是寻找无人认领行李的调查却很快取得了成果。

1月14日，警方发现了萨默顿男子的行李。这个行李箱被存放在阿德莱德中央火车站，寄存时间是11月30日（发现尸体的前一天）上午11点以后。

如果说凶手因为某种动机故意隐藏了萨默顿男子的身份的话，那么他似乎也对萨默顿男子的行李做了同样的处理。今天，人们会在行李箱的把手上用线或者塑料绳拴上名牌，然而在1948年，行李箱的名牌是用胶水贴在行李箱上的，非常不容易撕掉。然而，在警方发现的这个行李箱上，名牌却被撕掉了。因此，警方不仅无法确认萨默顿男子的身份，也无法知道他是从哪里来的。

这个行李箱中的物件就和本案的其他方面一样古怪。行李箱中的物件包括：

1件红色格子晨衣及腰带

1个洗衣袋［上面写着“基恩”（“Keane”）的字样］

1把装在保护套中的剪刀

1把装在保护套中的短餐刀

1把镂花刷子

4件背心［其中一件背心上的名字被扯掉了，另外一件背心上写着“基恩”（“Kean”）］

4条内裤（两条是三角裤，两条是普通内裤）

2条领带［其中一条领带上写着“T.基恩”（“T Keane”）的

字样]

1双红色毛毡拖鞋（鞋码是8号）

1条裤子，裤子上有干洗店或者洗衣店的标记，裤子的一个口袋里有6便士硬币，裤脚翻边里有沙子（意味着这条裤子也在沙滩上穿过）

1件运动外套

1件衬衫款式的外套

1条睡裤

4双袜子

1件黄色的衬衫款式的外套

1件名牌缺失的衬衣

6条手帕

1条围巾

1条轻型绳索

1个香烟打火机

8个大信封和1个小信封

2个挂衣服的衣架

1把剃刀和磨剃刀的皮带

1把刮胡刷

1把小螺丝刀

6支铅笔，其中3支是H铅笔（工程制图用铅笔）

1支牙刷以及牙膏

1个玻璃盘子

1个肥皂碟，其中有1个发夹，3个安全别针，1个前金属扣和1个

后金属扣（用来把领子固定在无领衬衣上），1个棕色纽扣，1个茶匙，1把坏了的剪刀，1板黄褐色（或者橘色）的线

1罐黄褐色（或者棕色）注鞋油

2张航空邮件贴纸

1块橡胶橡皮

在这些物件里，最明显的问题是：没有任何身份证明文件，没有钱（除了6便士硬币以外），也没有帽子（1948年那时候，男士是需要戴帽子的）。不管是在死者的身上还是在他的行李里，都找不到上述三样东西。死者行李箱里的物件十分普通，如果算上失踪的上述三样东西，这个行李箱里的东西几乎可以属于任何人。寄存这个行李箱的票根一直未被找到。那么，警方为何确定这个行李箱是萨默顿男子的行李呢？这个判断主要有以下几点依据：

1. 行李箱中的外套和死者身上穿的外套尺寸相似，行李箱中的外套只比死者身穿的外套尺寸稍小，这些外套的名牌都被撕掉了。

2. 行李箱中的衬衣尺寸与死者身上穿的衬衣尺寸相似。

3. 行李箱中的三角裤和死者身上穿的内裤品牌类似。

4. 行李箱中发现的手绢和死者身上的手绢类似。

5. 行李箱中的裤子和死者身上穿的裤子尺寸一致，长度也一致。

6. 最重要的一点是，警方在行李箱中发现的线是一个有力的证据。阿德莱德大学教授约翰·伯顿·克莱兰（John Burton Cleland）有些不情愿地在死因讨论环节中给出了以下的证言：“在行李箱中发现了一种橘色的亚麻线。在尸体身上和行李箱中的衣物上，我也发现了类似的线。行李箱中有一些橘色的线。通过显微镜检查，行李箱中的线在颜色和纤维粗细上都与行李箱中一条裤子口

袋的缝线类似，也与死者身上脱下的裤子上的纽扣用的缝线类似，还和修补死者外套领子所用的缝线类似。这些线的颜色是一种暖调的深褐色，这是一种并不常见的颜色。” ㊟

前5点联系都可能只是简单的巧合。这名身份不明的男子既不是特别高大，也不是特别矮小，因此另一个人的衣物也有可能正好与死者穿的尺码相符。然而，当前5点发现与第6点发现结合在一起时，就可以有力地证明这件行李是属于萨默顿男子的。此外，当时警方没有发现任何其他有可能属于萨默顿男子的行李箱。举个例子来说，如果当时警方发现了100件无人认领的行李，那么即便其中一件行李具备以上6点特征，也有可能完全是出于巧合，至少不能仅以衣服尺码相符这一点来判定行李箱就是萨默顿男子的物件。

总的来说，这个行李箱中的物件并没有告诉我们太多关于死者身份的信息。在1948年时，这个行李箱中的大部分物件都可能出现在任何一个在外旅行的男性旅客的行李箱中。格林伍德认为，行李箱中出现的镂花刷子、刀、螺丝刀、铅笔，以及剪刀都能够支持她关于“萨默顿男子是一名货船装卸指挥员”的理论。虽然货船装卸指挥员确实可能会携带上述这些工具，但是由于这些东西并不是特别专业的工具，所以也不能排除其他的可能性。

在这个行李箱里的物件中，有一条裤子上带有干洗店或者洗衣店留下的标记。这种标记是干洗店或者洗衣店为了防止客户衣物上的名牌脱落而画在衣物上用于确认客户身份的。也就是说，这个标记有可能是追踪死者身份的一条线索。在这条裤子上留下的标记为：1171/1、4393/7和3053/7。㊟ 一些在洗衣店工作的人士认为，这个标记应该是英格兰的某家洗衣店留下的，但是他们没有办法帮助警方进一步缩小洗衣店的范围。此外还有一些人在网上留言，表示他们认为这些标记事实上是某种密码。如果确实如此的话，那可真是一种相当奇怪的传递信息的方式了。关于那个年代的专业人士和业余人士如何使用各种秘密的方式传递

信息的故事我听得多了，如果真的存在这种“干洗店标记密码系统”的话，我相信我应该听说过这种东西才对。

有许多研究者花费了大量精力来追踪这条干洗店标记的线索。现代刑侦影视剧的发烧友往往相信，一条微不足道的线索可以给案件的侦破工作带来极大的转机，因此对他们而言，花大力气追踪这条线索似乎是一件完全合理的事。有人甚至把这条裤子上的干洗标记发表在了专业期刊——《干洗者期刊》（*Dry Cleaner's Journal*）上。他们希望这本杂志的某一位读者也许能找到在裤子上做标记的干洗店，然而这一努力并没有获得任何成果。

行李箱中的物件提供的最明显的线索是衣物上出现的名字：T Keane、Keane，以及Kean。然而值得注意的是，留有名字的这几件衣物都有一个共同的特点，那就是：没有办法在不损毁衣物的前提下去除这些名字。所以，也许这些名字与萨默顿男子的身份并无关系。格林伍德是一个土生土长的澳大利亚人，根据她的经验以及她的一些较年长的亲戚的经验，她在书中指出了这样一个事实：当二手衣物被转卖时，衣物上面常常会留有前任主人的名字。在20世纪40年代，因为衣服的价格比现在高得多，所以衣物上通常都会标有人的名字。在人们购入二手衣物以后，他们通常会用自己的名牌取代前任主人的名牌。

虽然警方并不能确定衣物上的名字是不是死者的名字，但是警方仍然根据这几个名字（T Keane、Keane，以及Kean）调查了关于死者身份的多种可能性。警方不仅调查了该姓名的若干种变体，比如Keanic、Kane、Tommy Reade等，甚至还考虑过名字首字母T代表阿拉伯语字母J的可能性。

一个新发现

负责侦查工作的警长利恩（Leane）将在行李箱中发现的衣物和死者身上穿的衣物一同交给阿德莱德大学病理学系荣誉教授约翰·伯顿·克

莱兰爵士。目前已经无法查到利恩警长究竟是哪一天将这些物品转交给克莱兰教授的，但是我们知道，在1949年4月19日，利恩警长从克莱兰教授那里得到了好消息。这一天，克莱兰教授向利恩警长提供了一个尸检时被漏下的重要发现。

1949年6月21日，在萨默顿男子的死因讨论会上，克莱兰教授在死者遇害时穿的裤子上发现了一条重要线索。正是这条重要线索最终引出了下文将要讨论的密码。克莱兰教授的证词如下：

> 在检查死者的衣物时，我在裤子的纽扣遮布右侧发现了一个很难找到的怀表袋，并从这个怀表袋中找到了一张纸。在发现这张纸之后，我又将其放回了怀表袋中。之后我花了很长时间才第二次找到了这张纸，因为死者裤子上的这个怀表袋是一个很容易就被忽略掉的口袋。㊟

有些媒体拿这个所谓的“秘密口袋”大做文章，将其渲染成某种只有间谍身上才有的暗袋。事实上，在那个年代中，这种暗袋是非常常见的。这种暗袋是用来装怀表的，而不是装间谍文件的。然而，在萨默顿男子案件中，也许后一种猜测更接近事实。在怀表袋中发现的这张纸状况良好，只是被卷了起来，纸上有“Tamam Shud”的字样。这几个字是印在纸上的，而不是手写或者用打字机打在纸上的，因此可以判断这张纸是从一本书上撕下来的。㊟这张纸被发现时状态良好，这说明这张纸是在死者死前不久才从书上撕下来的。如果这张纸已经在死者的怀表袋中装了几个月，那么纸张的破损程度应该更高一些。某些媒体报道中称纸上的字是“Taman Shud”，也就是把第一个单词的最后一个字母写成n，而不是m，这是一个广泛流传的错误说法。许多参考资料都将此案误作“Taman Shud”案。

在后文中，我将向读者详细解释这张奇怪的纸如何变成了本案的主要线索，并将一段密码引入了本案。现在我们先来看一看在这次死因讨

论会上出现的其他一些证据。

死因讨论会——寻找毒药

1949年6月17日至6月21日，警方举行了萨默顿男子案的死因讨论会。虽然在这次讨论会上，好几位专家提供了关于萨默顿男子死因的证言，但是这次会议并没有最终确认死者的死因。许多人都认为萨默顿男子死于某种毒药，然而这一论断既没有办法证实，也没有获得专家的一致支持。事实上，代理政府分析师罗伯特·詹姆斯·考恩（Robert James Cowan）认为，死者死于自然原因的概率比死于毒药的概率更高！此外，支持毒药说的人也没有办法指出死者究竟是死于哪种具体的毒药。

负责对萨默顿男子的尸体进行解剖的约翰·马修·德怀尔指出："死者脾脏特别大并且硬，有正常脾脏的3倍大。"[注]德怀尔还说："胃中有血，我认为这指向某种刺激性的毒药。然而在死者胃里的食物中，并没有发现我肉眼可见的异常物质。因此，我采集了死者胃、胃内容物、血液，以及尿液的样本，并对这几种样本进行了进一步的分析。"[注]

然而，德怀尔的上述怀疑却没有获得证实。德怀尔解释道："在我提交报告的时候，我认为毒药应该是巴比妥酸盐或者某种可溶性安眠药，直到现在我仍然认为这种猜测符合其他方面的发现。假设考恩博士确实没有发现任何巴比妥酸盐或者其他常见的毒药，我只能对这种情况表示万分惊讶，因为我认为他应该会发现的。我知道考恩博士是一名相当有经验的化学家，因此如果他没有发现任何毒药，那么我接受他得出的这一结果。"[注]

虽然德怀尔发表了上述声明，但是他仍表示很难相信致死剂量的毒药竟然未能在测试中显现出来。经过一番进一步的讨论以后，德怀尔提出了与上述说法相矛盾的总结陈词："总的来说，我相信巴比妥酸盐可能并不是致死的原因。但是，正如我早先所说的那样，巴比妥酸盐是一

种可能的解释。我个人的意见是，基于化学家的发现，我们可以说巴比妥酸盐不太可能是死者的死因。然而如果要做出最大限度的推测的话，我认为我起先怀疑的死因仍有可能是死者的真实死因。”[注]

关于巴比妥酸盐的问题，克莱兰教授也表示了与德怀尔类似的惊讶。克莱兰教授的证言是：“除了巴比妥酸盐这个特例以外，普通人应该不知道其他通过分析也无法被发现的毒药。”[注]

接着，考恩博士提交了他对多种样本的分析结果（包括死者胃、胃内容物、肝脏、肌肉、血液，以及尿液的样本）。考恩表示：“我对各种常见毒药进行了测试。最常见的毒药包括氰化物、生物碱、巴比妥酸盐、石炭酸。如果死者死于我检测过的任何一种毒药，并且这种毒药是口服进入体内的话，死者体内就肯定能找到这种毒药的痕迹。”[注]此前的其他证言显示，在死者的遗体上没有发现任何针孔。考恩是唯一不同意毒杀说的人。虽然考恩从未说过他进行的检测能排除所有少见的毒药致死的可能性，但是他表达的意见是：死者死于自然原因的概率高于他死于某种很少用于自杀和他杀的罕见毒药的概率。

而克莱兰的结论则与考恩医生完全相反，他认为：“几乎可以确定死者不是自然死亡。死者很可能是出于自杀的意图而服下了某种毒药。”[注]然而，由于并没有发现死者有呕吐的痕迹，克莱兰对此表示不安，他指出：“大部分常见的毒药都会导致服药人出现呕吐或某种程度的抽搐，这些情况会使得死者引起他人的注意。”[注]

考虑到本章的下一个案件的情况，我需要提醒读者注意克莱兰在死因讨论会上排除的另外一种毒药：“氰化物致死速度很快，然而在现场没有发现任何瓶子，也没有人闻到氰化物的气味。”[注]而关于巴比妥酸盐，克莱兰则提出了与德怀尔类似的意见：“巴比妥酸盐可能是致死的原因，如果我们能在死者的样本中发现巴比妥酸盐的话。”[注]从克莱兰的证言中，我们可以感受到他内心的焦灼，他的处境就好像一个人发现了一头方的猪，却找不到方的洞，只有一个圆的洞，因此他只能不断地

想尽办法把这头方的猪塞进圆的洞里去。

在这次死因讨论会上，塞德里克·斯坦顿·希克斯（Cedric Stanton Hicks）爵士提供的证言最有趣，也为我们提供了一种可能的解释。希克斯显然想到了一种与证据相吻合的毒药，但是他却选择用一种非常迂回曲折的方法来提示出这种毒药的名字。希克斯爵士首先开了一个玩笑，他说：“当大家都说死因是巴比妥酸盐，但是在死者体内又找不到巴比妥酸盐时，毒药就肯定是索佛那[注]。”[注]然而，接下来希克斯爵士又开始解释为什么本案的毒药并不是索佛那。

最后，希克斯终于说出了他心中的答案，却是以一种十分隐晦的方式。他说：“因此我倾向于认为，死者使用的可能是一类阻止心脏收缩的药物。证物第一个词是该类药物的名字，其他的词是这类药物中具体药物的名字。”[注]所以参加死因讨论会的人都不得不抬头看布克斯出示的证物。希克斯并没有说出毒药的名字，而是把它写了下来，并且作为一件证物拿出来给大家看！为什么希克斯爵士要采取这种间接的方式呢？读者很快就会明白了。

希克斯接下来的证言是：“在这类药物中，第一种药有几种不同的形式，而我个人更倾向于第二种药物。第二种药物只需要相对较小的剂量就能产生极大的毒性，我的意思是说即使是口服的话，也是这样。而且，已经进行的毒物测试都没有办法检测到这种药物。即使尸检人员一开始就怀疑这种药物，它也是极其难以检测到，甚至是不可能检测到的。我的意思是说，常见的化学测试没有办法检测到这种药物。而普通人就能够很容易地取得这种药物，不需要什么特殊的途径。”[注]

虽然在所有证人的证言中，希克斯的证言似乎是最可信的，然而他也对自己的结论表示出了一定程度的怀疑。他说：“我对自己的结论很有信心，然而只有一点与我的结论不相符合，那就是没有呕吐的痕迹。然而，不同的人服下这种药物之后的反应会有所不同，或者死者也许曾在其他地点呕吐过，后来才到了海堤边。但是我承认，如果能在某处发现死者呕吐的痕迹，我会对这个结论更加有信心。”[注]

希克斯之所以要通过如此隐晦的方式提出毒药的名字，是因为他担心某些心怀恶意的人从讨论会的记录文件中读到他的证言以后，会利用这个知识实施无可挽回的谋杀。托马斯·克莱兰负责写本次死因讨论会的简要总结，他一开始也采取了和希克斯同样的做法。克莱兰写道："斯坦顿·希克斯爵士能想到的唯一一种与尸检结果相符的毒药是他在讨论会上提到的某一类毒药中的一种。然而，这种毒药也会给我们带来一些困难。死者并没有呕吐的痕迹，虽然一些证据能证明死者可能曾经出现过抽搐的情况。" [注]接下来，克莱兰写道："我能够接受死者死于毒药的解释。并且这种毒药很可能是一种葡萄糖苷，死者很可能自己施用了这种毒药，或者其他人对死者施用了这种毒药。" [注]据此我们终于知道，斯坦顿·希克斯爵士不愿说出口的那类毒药就是葡萄糖苷！克莱兰在这份总结中并没有写出希克斯在证物中列出的两种具体药物的名字，但是这两种药物其实是洋地黄苷和毒毛花苷。

案发将近10年以后，萨默顿男子案的最后一次调查会于1958年3月14日结束。在这次调查会的记录中，我们可以看到这样的陈述："我无法确定死者是如何死去的，也无法确定死因是什么。" [注]

虽然警方曾经采集过死者的尿液、血液、肝脏、肌肉，以及胃内容物的样本，并对这些样本进行了检测，但是，存放这些样本的停尸房后来被关闭，并且停尸房的所有活动都移到其他地点，而这些样本也随之丢失了。因此，我们现在无法使用更加先进的化学测试来检测上述样本。幸运的是，死者指纹的样本仍然存在，然而时间已经过去了这么久，通过指纹线索找到萨默顿男子身份的可能性已经很低了。既然在当时的数据库中查不到与该指纹匹配的人，现在恐怕也很难查到。而且，很难想象指纹这条信息能对萨默顿男子的死因提供什么线索（即使是间接线索）。

即便我们接受萨默顿男子被毒死的理论，警方掌握的线索也无法让调查会上的任何一名证人准确地判断出死者究竟是死于谋杀还是自杀。如果他是死于谋杀，那么毒药是通过何种方式进入死者体内的呢？从尸

检的结果来看，死者胃里的食物是馅饼，那么死者吃下最后一餐时是否被下了毒呢？格林伍德分析过死者可能吃下馅饼的地点，她认为可选的地点并不多：包括格莱内尔格火车站的馅饼推车、某处私人住宅，或者残疾儿童之家。但是逐一分析完上述这些结果以后，格林伍德并没有找到什么有用的线索，并且她自己也承认，很难想象残疾儿童之家会是“杀人犯或者秘密间谍的庇护所”。[注]也许，死者的最后一餐并没有毒。那会不会是他的香烟被下了毒呢？为什么死者身上的同一包香烟里有两种不同的香烟？警方显然从未认真检查和分析过死者身上的香烟，似乎他们从未考虑过香烟中有毒的可能性。

遗憾的是，现在已经没有办法再对这些香烟进行检测了。这些香烟就和从死者身上取得的组织样本一样在很久以前就丢失了。事实上，萨默顿男子案的大部分证据如今都已经不存在了。有些物件（比如行李箱以及行李箱中的东西）已经被毁，另一些证据则是被意外遗失了。[注]甚至连警方当时建立的关于本案的卷宗也找不到了。2002年，有人发现了这份卷宗的一小部分。证据损毁和丢失的现象让我们想起了本书第4章中写过的黄道十二宫杀手案。但是，在萨默顿男子案中发生这种证据丢失的情况相对来说是可以理解的，毕竟此案已经过去了很长时间。

萨默顿男子的墓碑

假如在死因讨论会上出现任何疑点要求对死者重新进行尸检，那么警方就必须向法院申请掘尸重验的手续，因为萨默顿男子的尸体已经于1949年6月14日下葬。南澳大利亚格兰德斯坦德博彩业协会支付了萨默顿男子葬礼的开支。一开始，萨默顿男子的坟墓上插有一个木质十字架，十字架上写着“不知名的萨默顿男子”。但这个十字架很快被如图6–5所示的墓碑取代了。

虽然十字架上只写着一个人，但是这座坟墓中实际上有三具尸体。根据规定，墓地可以在租期满后将其他人的尸体埋在原来的尸体上方，

并且变换墓碑。

在葬礼后不久，又出现了两张萨默顿男子的新照片，并且有人对萨默顿男子的头部和肩部进行了铸型，以便造出萨默顿男子的半身像。从图6–6中可以看出，这组新照片与原始照片出入不小，这是因为照相时死者的尸体已经被保存了较长时间。在这组新照片上，萨默顿男子甚至还戴了一条和原始照片中不同的领带！此外，我们还知道，由于铸型时尸体已经被存放了很久，所以萨默顿男子的半身像与死者的真实样貌也不是特别接近。



图6-5 这名身份不明的男子的墓碑。图中文字：在此处安息的是1948年12月1日被发现于萨默顿海滩上的无名男子



图6-6 这名身份不明的男子的更多照片

萨默顿男子的半身像完成以后被保存在南澳大利亚博物馆中。之所

以要在博物馆中陈列这座半身像，是因为有人相信，在未来的某一天，也许会有人能够认出这名男子，并最终确认他的身份。下文中，我们还会继续谈到这一点。

《鲁拜集》中的密码

在向读者介绍讨论会上的情况之前，我曾经提到克莱兰博士在死者身上的暗袋中发现了一张写有“Tamam Shud”字样的纸片。一开始，这张纸片上的文字令警方大惑不解。最终，博学的弗兰克·肯尼迪（Frank Kennedy）指出，波斯诗人欧玛尔·海亚姆（Omar Khayyám）的诗集《鲁拜集》（*The Rubaiyat*）的某个版本的最后几个字就是“Tamam Shud”，而其他版本的最后几个字是“Tamam”。在一些图书馆管理员的帮助下，警方得知“Tamam Shud”源自波斯语，可以翻译为“已结束”“已完结”，或者“将结束”“将完结”。

伦纳德·道格拉斯·布朗（Leonard Douglas Brown）警探对《鲁拜集》的内容进行了以下的总结：

> 诗歌本身的意思是：我们知道这个世界为我们准备了什么，但不知道另一个世界为我们准备了什么；当我们在这个世界上生存时，我们应该尽情地享受生活；而当离开的时刻到来时，我们也应该毫无遗憾地离开。(注)

这本书的主题似乎为自杀说提供了一定的支持。但是，如果萨默顿男子死于自杀的话，他为什么不随身带着《鲁拜集》作为自己的遗书呢？把写有“Tamam Shud”字样的纸放在那么隐蔽的暗袋中，很可能根本不会有人发现（事实上，警方就差点儿没能发现这张纸！）。就算有人发现了这张纸，也未必能把这两个词和《鲁拜集》联系到一起。如果一位自杀者只是想让世人知道他离开这个世界毫无遗憾，那他为什么要

选择这样一种隐晦的方式来表达这一点呢？

在萨默顿男子的葬礼和死因讨论会结束以后，警方公开发动群众帮忙寻找这本特殊的《鲁拜集》，也就是写有“Tamam Shud”字样的纸张的来源。在征求公众的协助之前，警方已经搜寻过《鲁拜集》，但是没有获得成功。事实上，问题比警方预想的要困难得多，因为《鲁拜集》在当时是一本非常流行的书。

虽然《鲁拜集》最初是由波斯诗人欧玛尔·海亚姆（1048—1131）于萨默顿男子死去的800多年前写成的，但是这本书在19世纪被爱德华·菲茨杰拉德（Edward Fitzgerald）翻译成英文后才变得流行起来。澳大利亚的几乎每个图书馆中都有这本书。书店里也能够找到不同版本的《鲁拜集》，人们家中更是藏有不计其数的《鲁拜集》。费尔特斯甚至推测“《鲁拜集》可能是当时阅读人数最多、讨论人数最多的书籍之一”，[注]而且可能是“史上最畅销的英语诗集”。[注]尽管困难重重，警方还是展开了对这本《鲁拜集》的搜寻。他们对全国所有图书馆馆藏的《鲁拜集》都进行了检查，确认“Tamam Shud”两个词有没有被撕去。因为如果能确认死者身上的纸片来自某个图书馆的话，图书馆的位置也许能为本案提供一些线索。可惜上述努力并没有获得成果。然而，警方并没有放弃。根据死者身上发现的纸片的形状，警方复原了印有这个字样的书页，并向公众公布了这份复原图。警方希望某位看到此图的民众能够帮助警方找到那本被撕去了两个词的《鲁拜集》。

7月22日，一名商人[注]看到了警方公布的复原图，并查看了自己持有的《鲁拜集》。我之所以使用“持有”一词，是因为这位商人手上的《鲁拜集》其实并不是他的。几个月前，这位商人的妹夫曾经搭过商人的车，并把这本《鲁拜集》落在了该车的手套箱中。这一天恰好就是萨默顿男子的尸体被发现的那天！这位商人发现，自己手中的《鲁拜集》正是警方在寻找的那本，于是他打电话给自己的妹夫询问此事。但是他的妹夫却否认这本《鲁拜集》是自己留下的。妹夫称，当天他只是在车后座前方的地面上发现了这本书，他以为这本书是车主的，于是就把它

捡起来放进了仪表盘上的手套箱中。第二天早晨，这位商人给警方打了电话汇报了此事。

警方的专家用显微镜比较了死者身上的纸片和商人找到的这本《鲁拜集》，检验结果和预想的一样——写有“Tamam Shud”字样的纸片确实是从这本《鲁拜集》上撕下来的。注

虽然《鲁拜集》是一本当时非常常见的书，但是这本被撕去一角的《鲁拜集》却是一种非常罕见的版本。事实上，在爱德华·菲茨杰拉德把《鲁拜集》译成英文以后，这本书并没有立即流行起来。而这本被撕去一角的《鲁拜集》是第一版，出版商是新西兰的惠特科姆和图姆斯（Whitcombe & Tombs）出版社。注这本与萨默顿男子案有关的《鲁拜集》也于20世纪50年代丢失，在今天的所有研究者中，再也没有人能找到完全一样的版本了。格里·费尔特斯曾于1964—2004年在南澳大利亚警察队伍中工作，他专门撰写了一本关于萨默顿男子案的书，此书对萨默顿男子案的介绍是所有书籍中最详细的。费尔特斯曾花大量精力寻找上述版本的《鲁拜集》，然而，就连他也找不到一本和本案中完全一样的《鲁拜集》。费尔特斯找到了两本由惠特科姆和图姆斯出版社出版的第一版《鲁拜集》。但是这两本和萨默顿男子案中的那本也不完全一样。其中一本的字体不同，而且结尾处没有“Tamam Shud”两词。费尔特斯表示，他并不确定这本书是不是他想找的版本。这本书可能是新西兰的第一版《鲁拜集》，也可能是由柯林斯出版社（Collins Press）出版的英格兰的第一版《鲁拜集》——后一版本在英格兰印刷，然后被运到澳大利亚分销。早在上文中的那位商人发现萨默顿男子案中的那本《鲁拜集》之前，一位警官就曾怀疑死者身上的纸条来自这一英格兰版本。让事情变得更加复杂的是，即使同样是“第一版”，也有若干不同的印刷批次，每个批次印的书都可能有一些不同。甚至同一个印次的书也未必完全一样。比如，在图书印刷的过程中，出版商可能会发现一些小错误（比如小笔误），此时出版商就会停止印刷来修正这个错误。虽然同一印次的书之间差异通常很小，但是同一版本不同印次的书则有可能

出现较明显的差异：比如使用的纸张不同，或者存在其他一些较容易注意到的区别。

萨默顿男子案中的这本《鲁拜集》还为此案的调查者准备了一些其他“惊喜”。其中之一是，这本书的背面有一段手写的密码。[注]为了搞清楚这段密码的意义，我们必须做一些研究。

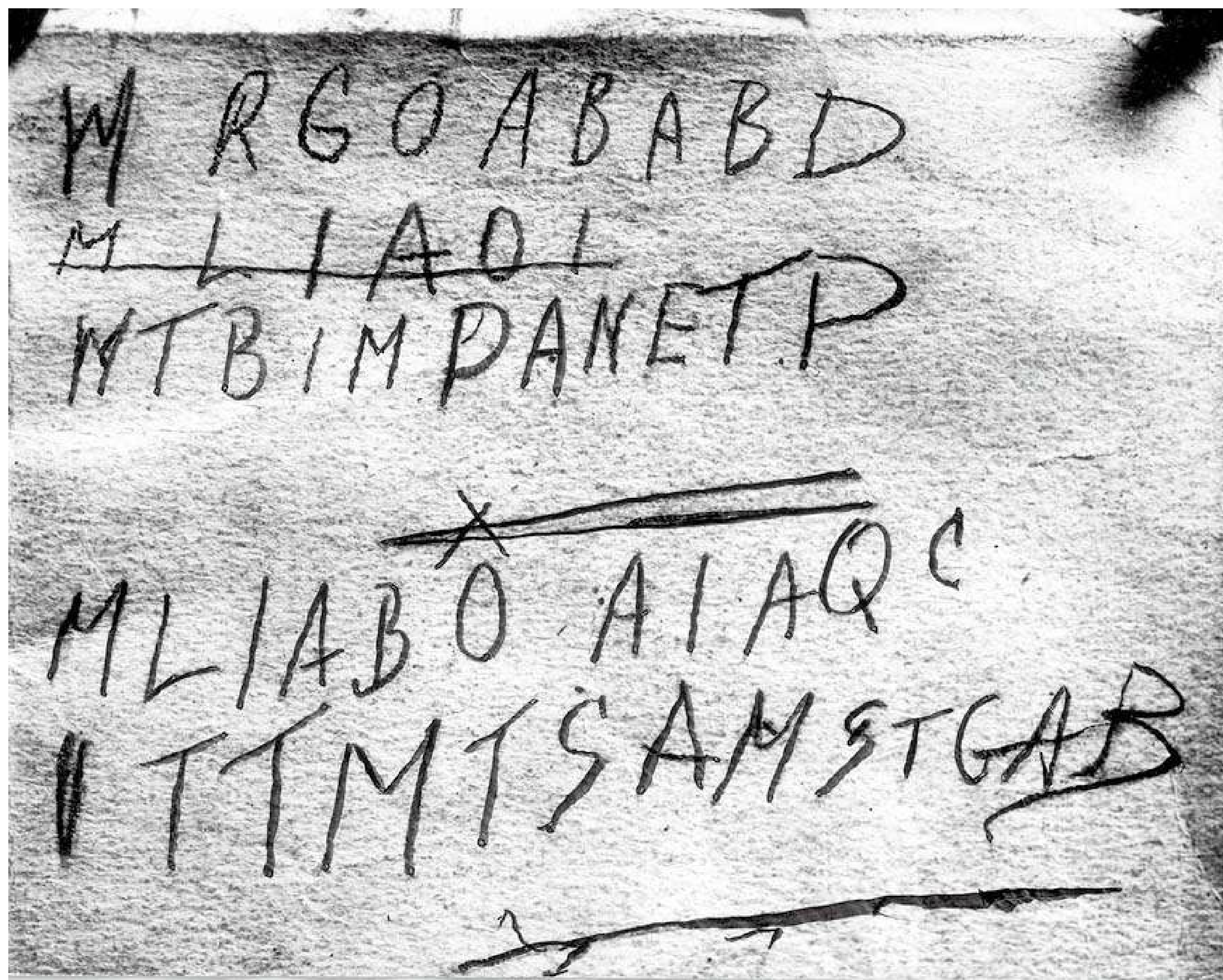


图6-7 与这名身份不明的男子有关的密码

密码的第2行画了一条横线，写密码的人有可能是想用下划线强调这行内容，也可能是划掉了这行的内容。因为第2行的内容和第4行的内容非常类似，所以也许是第2行写错了，划掉第2行，重新在第4行写下了正确的内容。以下这个事实可以支持上述猜测：如果忽略第2行，那么在所有其他行的文字中，只要出现字母A，下一个字母就有一半情况

是字母B。如果这些字母是随机的，就不太可能出现这种情况。从另一个角度来看：字母B在这段密码中出现了5次，其中4次是紧跟在字母A后面。因此，我相信写密码的人在第2行中写错了，所以他划掉了第2行，而把正确的内容写在了第4行中。

假设我们忽略被划掉的第2行，再确定其他几个不清楚的字母，比如第一个字母就不太清楚，这个字母既像是W又像是M（我认为是W，因为这段密码中的其他M写得挺清楚的，而第一个字母和那几个M并不类似）；再比如字母O上面的X（难道是抱抱亲亲的意思？(注)），剔除这个X，这段密码的内容就变成了：

WRGOABABD

WTBIMPANETP

MLIABOAIAQC

ITTMTSAMSTGAB

对这段文字中的每个字母进行频率统计，得到：

A = 8	G = 2	M = 4	S = 2	Y = 0
B = 5	H = 0	N = 1	T = 6	Z = 0
C = 1	I = 4	O = 2	U = 0	
D = 1	J = 0	P = 2	V = 0	
E = 1	K = 0	Q = 1	W = 2	
F = 0	L = 1	R = 1	X = 0	

在本书的第1章中，我已经向读者展示过，在破译简单的密码时，

字母频率统计是一件非常有用的工具。比如，读者可能还记得，在英语中，字母E出现的概率高达12.7%，比其他字母都高出很多。但如果我们只统计每个单词的首字母，那么在正常英语中出现概率最高的字母就变成了T，而字母E作为单词首字母出现的概率只有2.8%。由此我们可以看出，一个给定的字母在单词不同位置上出现的频率会有所不同。

如果我们只统计每个单词的最后一个字母，那么字母E又成了出现概率最高的字母。在正常英语中，有22.3%的单词以字母E结尾。

在图6–8中，我们可以看到英语中的26个字母出现在单词不同位置上的概率。

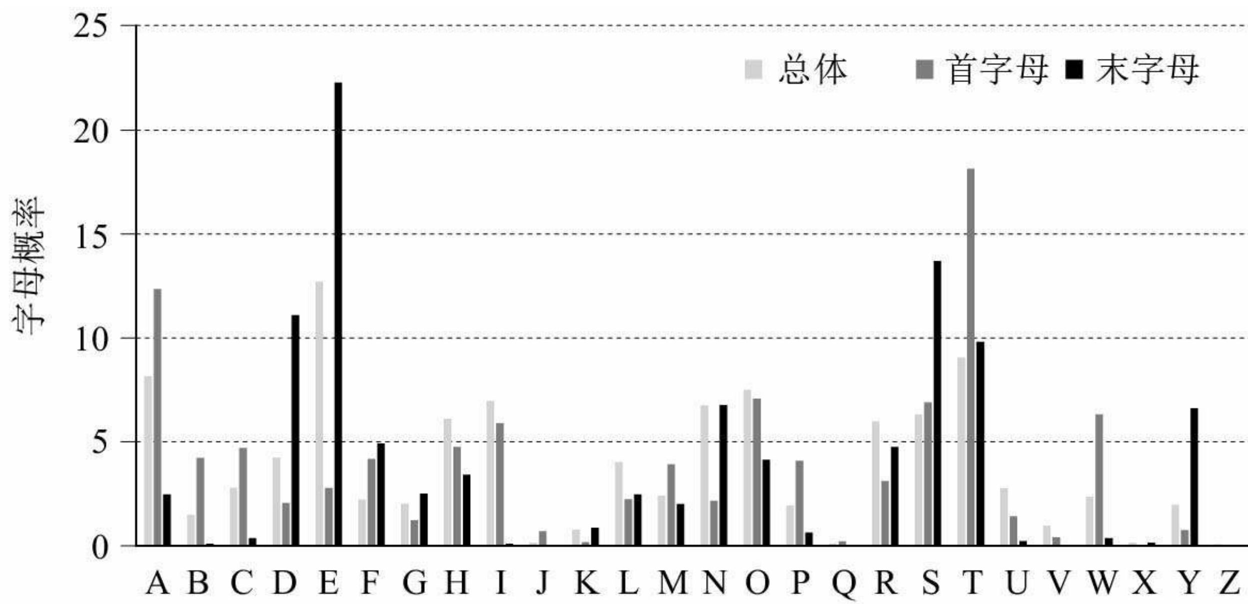


图6-8 字母概率：总体（浅色），首字母（中间色），末字母（深色）

图6–8描述的是在英语单词的不同位置上各字母出现概率的高低。有些字母在单词不同位置上出现的概率相差很大。比如字母E和字母S——这两个字母出现在词尾的概率比出现在其他位置上的概率高很多。而字母A和字母T出现在单词开头的概率比出现在其他位置上的概率高很多。

现在，我们把《鲁拜集》上的这段密码中各字母出现的频率和图6–8中各字母的出现概率进行比较。首先，我们比较字母出现在单词所有

位置上的概率（图6–9）。

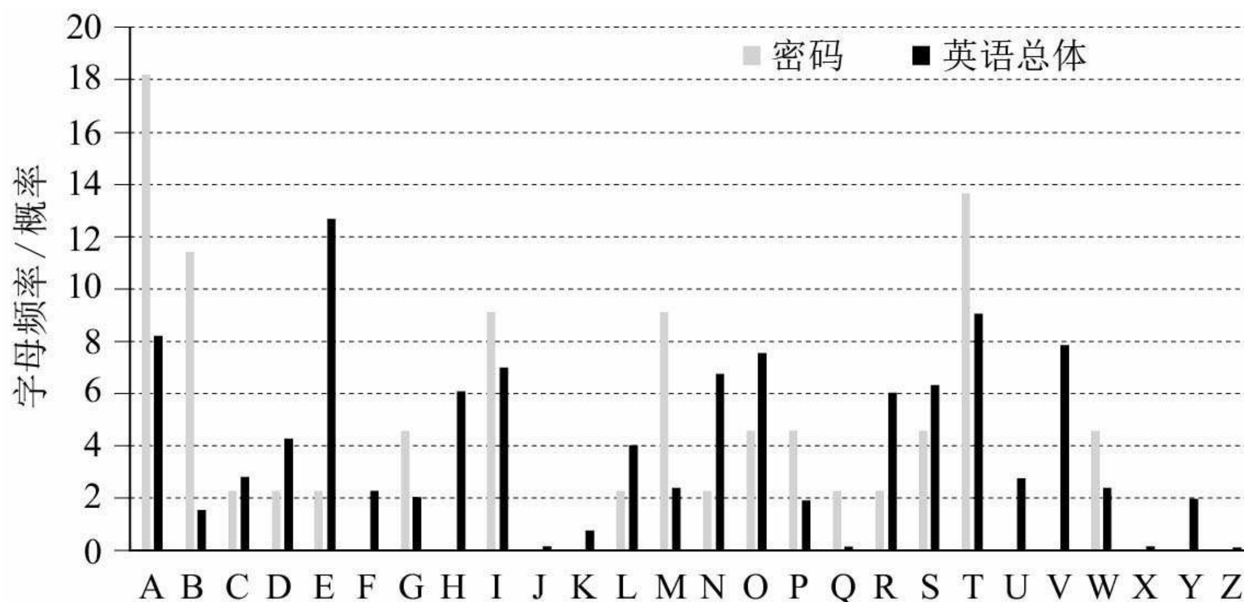


图6-9 密码字母频率（浅色）和英语总体字母概率（深色）的对比

从图6–9中可以看出，浅色柱和深色柱相差很大，这说明密码并不是用正常英语写成的。因此我们可以排除换位重排密码的可能性（比如第5章中提到的IRA密码就是换位重排密码）。如果加密的方式仅仅是把明文中字母的顺序改变，那么各字母出现的频率就不会改变，图6–9中的各个浅色柱就应该与深色柱高度大致相同。

既然排除了换位重排密码，也许我们可以假设这段密码是某种替代密码。但是在得出结论之前，我们还需要再比较分析一下。

在下页图（图6–10）中，我们比较了密码中的字母频率和英语文字中单词首字母的字母概率。

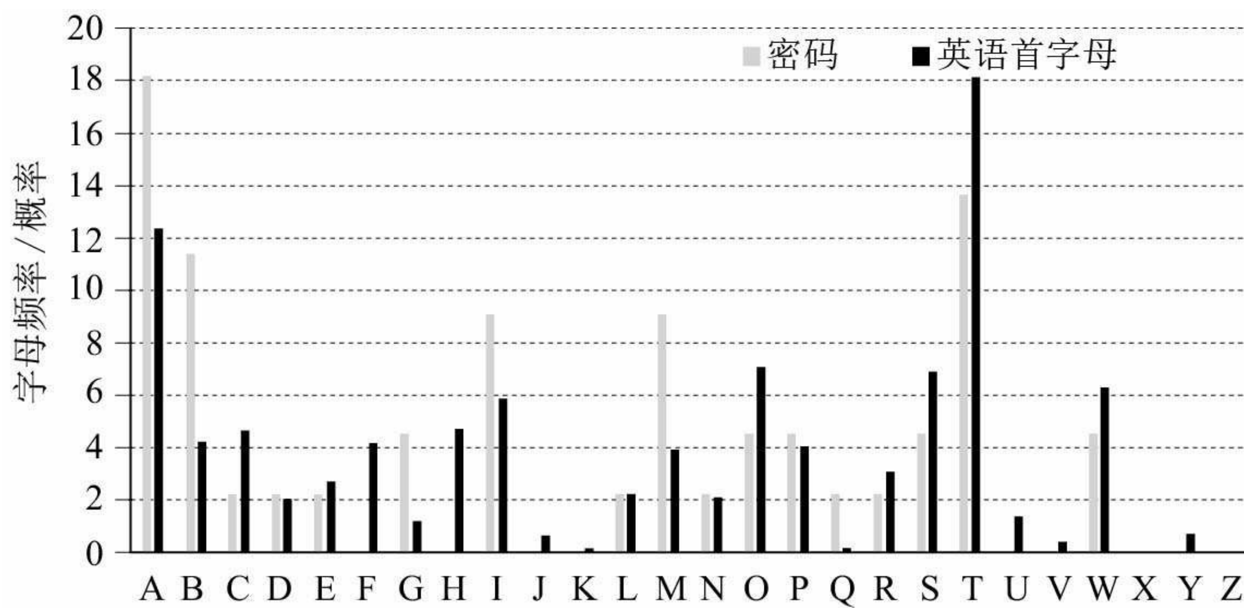


图6-10 密码字母频率（浅色）与英语单词首字母字母概率（深色）的对比

图6–10中的浅色柱和深色柱的匹配程度要比上一张图（图6–9）高得多。比如，在上一张图（图6–9）中，字母E对应的浅色柱和深色柱相差很远，但是在图6–10中，字母E对应的浅色柱和深色柱则高度相当。

最后，我们比较一下密码中的字母频率和英语单词中末字母的概率，比较的结果见图6–11。在图6–11中，浅色柱和深色柱的匹配程度要比上两张图都差！(注)

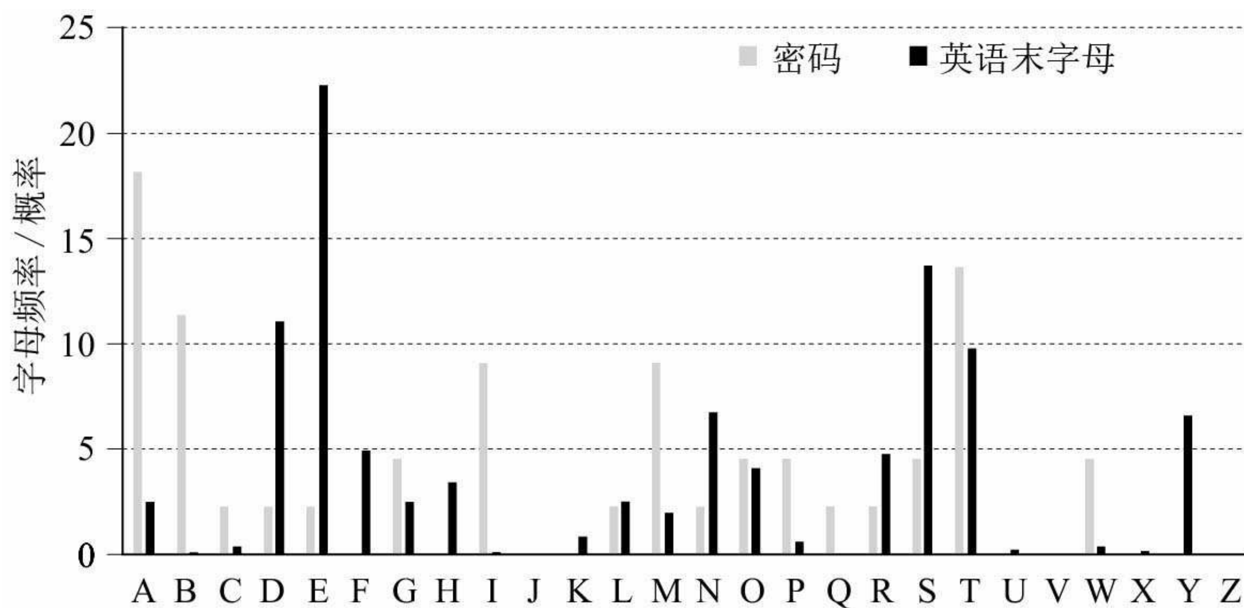


图6-11 密码字母频率（浅色）与英语末字母字母概率（深色）的对比

密文中的字母概率和英语明文单词首字母的概率匹配度较高，这种情况使得许多专家相信，这段密码其实是首字母缩写——类似于今天我们使用的LOL（laugh out loud，意为：大笑出声），ROTFL（rolling on the floor laughing，意为：笑得满地打滚），IMHO（in my humble opinion，意为：鄙人的意见），WTF（what the fuck，意为：什么鬼东西）等。我还可以给读者举一个更古老的首字母缩写的例子，那就是INRI。(注)

之所以很多人都认识上面这些首字母缩写，是因为它们已经成了标准用法。然而，如果一段首字母缩写并不常见，要解读它的意思可能会相当困难，而且对同一段缩写几乎总是可以找到多重解读。下面，我将为读者列出一些首字母缩写，这些缩写的流行程度各不相同。你能认出或者猜出几种缩写的意思吗？在这些缩写中，有的缩写有不止一种被广泛接受的意思。中间有点号的缩写其实是麦克·霍金（MC Hawking）的一首歌曲的名字。

AFAIK

AFC

ANFSCD

AWGTHTGTATA

AYBABTU

BBW

BFD

BICBW

BRBGTP

BTDT

CIO

CYA

DIIK

DILLIGAD

DIY

DMML

EMML

F2F

FCOL

FIGMO

FOAF

FTW

FWIW

F.Y.M.A.S.M.D.

GMAB

GMTA

HMFIC

HSIK

IBTD

ICYDK

IYD

JIC

KUTGW

LIRGAS

LOML

MCIBTY

MTFBWY

NAGI

NBTD

NSFW

OFS

OP

PDQ

PITA

QED

RTFM

SOL

SSEWBA

STBY

TAF

TGAL

TMI

UIAM

VFM

WAEF

WYP

XAO

YBYSA

YHTBT

ZA

以上所有缩写词的意义都可以在以下网址上找到（除了那首歌的歌名）：https://web.archive.org/web/20151108174013/和http://www.gaarde.org /acronyms/?lookup=A-Z。有兴趣的读者可以自行查看。

有时候，可以把这种首字母缩写词连成很长的一串。以下是一个极端的例子，这是《腓尼基人》杂志给读者出的一道难题，之前提到，《腓尼基人》杂志的读者群是美国国家安全局的退休人员。㊟

Can NSA (or The Phoenix Society) Crack This Code??

When teen-age idol Justin Bieber used Twitter to tweet the recording of "At Last" by 13-year-old **Madison Beer** & say "She can sing. Great job," her tweeted response was:

OMGOGMFHAHDBSBAWHEBSBSHHWEHHDXHSHHAFBBAGEEHYBT
I CANT BELIEVE THIS IS HAPPENING. I AM CRYING.

The Phoenician editor (who spent some time as a cryppie) had no trouble reading the last 9 words & suspects the first 3 letters of the first part stand "Oh, my gosh!" (or words to the effect) & that the underlying message is in English. But, being one of the few people in the world without a cell phone, he doesn't speak Twitter & has no idea what the next 43 characters stand for. Can some younger person who regularly texts messages tell him what OGMFHAHDBSBAWHEBSBHHWEHHDXHSHHAFB GEEHYBT means? As we said, he doesn't know (& we are sure there are other readers who might appreciate getting the words) .

Please send in your suggestions (even if it's only 3 or 4 letters) to Editor Harry Rosenbluh at **hulbnesor@verizon.net,** or to his Laurel address (back on the **ifc** page), or leave your translation (& name) on his phone answering machine at **301-**

10Q!

THE PHOENICIAN 16 WINTER '12-13

图6-12 对专业人员发起的挑战

图中文字翻译如下：

美国国家安全局（或者菲尼克斯协会）能够解开这段密码吗？

青少年偶像贾斯廷·比伯（Justin Bieber）在推特上转发了一段视频，视频的内容是13岁的麦迪逊·比尔（Madison Beer）在唱《最后》（At Last）。贾斯廷·比伯在转发时还评论道：“她确实会唱歌。唱得很好。”然后，麦迪逊·比尔回复了如下内容：

OMGOGMFHAHDBSBAWHEBSBSHHWEHHDXHSHHAFB

我无法相信贾斯廷居然转发了这个！我都哭了。

作为《腓尼基人》的编辑（以前我也解过密码），最后一句话

很容易读懂，但我怀疑前3个字母代表“Oh，my gosh（哦，我的上帝）”（或者意思相同的其他几个字），我还认为这段密码可能是用英语写成的。然而，由于我是现在这个世界上少数几个连手机都没有的人，更不会说推特流行语，所以我完全不知道后面的43个字母到底是什么意思。有没有哪位年纪较轻、经常发短信的人能告诉我“OGMFHAHDBSBAWHEBSBSHHWEHHDXHSHHAFBBAGEEHYBT”究竟是什么意思呢？我已经说了，我看不懂这段密码（而且我很确定还有其他读者也看不懂，他们可能也想知道这段密码是什么意思）。

请把你的解法（即使只有3或4个字母）发给哈里·罗森布拉（Harry Rosenbluh）编辑。罗森布拉编辑的电子邮箱地址是hulbnesor@verizon.net。你也可以将答案寄到编辑的地址（地址详见后面的网页），或者打电话将你的解法和姓名留在罗森布拉编辑的语音信箱中。罗森布拉编辑的电话是301－……

谢谢！

关于《鲁拜集》中的这段密码的性质，我的结论是：这段密码就是一串单词的首字母。澳大利亚的海军情报机构以及密码专家吉姆·吉洛格利（在前文中我们提到他在破译IRA密码方面的成就）也得到了与我一样的结论。在《未解之谜（下）》的第7章和第9章中，读者还会再次看到吉姆·吉洛格利的名字。畅销书《码书》（*The Code Book*）[注]的作者西蒙·辛格（Simon Singh）也认为萨默顿男子案的密码就是首字母缩写。

吉洛格利提出了部分密码示例解法：

MLIABO = My Life Is A Bundle Of（我的生活是一束）

ITTM = I Think That My（我想我的）

而格里·费尔特斯给出的解法则是[注]：

ITTMTSAMSG = It’s Time To Move To South Australia Moseley Street Glenelg **（是时候搬去南澳大利亚州格莱内尔格镇的莫斯利街了。）**

问题在于，首字母缩写可以产生出许多不同的解法。如果读者试着破译前面的那60个首字缩写密码，你就会发现其中有些你见过的缩写比较容易看出意思，而另一些首字母则可以有几种不同的解读。然而，在破译萨默顿男子密码时，并没有任何约定俗成的缩写用法能够帮助我们。也许这段密码对于萨默顿男子以外的任何人都没有意义，或者仅对和萨默顿男子很亲密的一两个人有意义（然而这一两个人却不愿意，或者不能出来指认萨默顿男子的身份）。因此，在破译这段密码时，你给出的解法与其说是反映了萨默顿男子的信息，不如说是反映了你自己的信息。当我们把密码中的这些字母看作单词的首字母，并靠个人想象进行补充的时候，你的潜意识便会开始工作，扩充出各种你能想到的信息，这就相当于密码版本的罗夏克墨迹测验。[注]

虽然萨默顿男子密码的字母概率特征强烈支持我的假说（即密码是一串单词的首字母），但也有其他一些研究者认为这段密码使用的是其他加密系统，并试图以此为假设破译这段密码。

在格里·费尔特斯所著的关于萨默顿男子案的书中，作者花了17页的篇幅专门讲述不同的研究者破译这段密码的方法。[注]这些方法五花八门、错综复杂、令人费解，而且看起来都不正确。根据费尔特斯的说法，这类解法还有许多，他因为受篇幅所限才没能列出更多。对这些解法有兴趣的读者可以去阅读费尔特斯的参考文献。在本书结尾处，我还列出了一些YouTube网站上的视频链接以及其他一些网址，这些都是阿德莱德大学的教授和学生试图破译萨默顿男子密码而做的一些工作。

在这里，我要向读者介绍两名阿德莱德大学学生的一项工作。露西·格里菲斯（Lucy Griffith）和彼得·瓦索斯（Peter Varsos）在德里克·阿博特（Derek Abbott）教授和马修·贝里曼（Matthew Berryman）博士的

指导下研究了这样一种可能性：萨默顿男子密码的作者是否有可能使用《鲁拜集》作为“一次性密码本”来进行加密？当然，“一次性密码本”中的文字应该是随机的，而不应该是有意义的英文文字。因此，他们研究的问题准确来说不叫“一次性密码本”，而应该叫作“滚动密钥密码”。不过，不管怎么样，这项研究最终并没有取得喜人的成果。即便萨默顿男子密码真的是通过这种方式创造出来的（我个人相当怀疑这一点），我认为他们的这种研究方式也很难取得成果，因为他们手中的《鲁拜集》与萨默顿男子案中的那本并不是同一版本。虽然我个人并不相信《鲁拜集》与我们讨论的密码有任何联系，但这本书却可能与其他密码有关。

如果萨默顿男子的身份是一名间谍的话，这样一本罕见版本的《鲁拜集》绝对是创造书本密码的理想工具。在《未解之谜（下）》的第9章中，我将向读者详细介绍这类与比尔密码相关的书本密码。就目前的内容而言，读者只需要理解以下几点：在书本密码中，被当作加密工具的书籍必须比较少见，但又不能引起他人怀疑。此外，密码的发送者和接收者都需要有这本书，两本书必须完全一样，因为这本书就是密码的密钥。

不管这本《鲁拜集》是否确实曾被用来创造或者破译密码，有一个事实可以支持这本书被当作密钥使用的假说，那就是：在与萨默顿男子有联系的物件中，所有物件都只有实用功能，而这本《鲁拜集》是唯一的例外。也许萨默顿男子曾有过地址簿，或者家人和朋友的照片，但我们从未找到这类物件，也许它们被凶手偷走了。关于萨默顿男子的个性，这本《鲁拜集》是我们掌握的唯一线索。然而，由于这本书在当时是一本非常流行的书，所以这条线索也没有太高的价值。在前文中我们已经提到，与萨默顿男子案相关的这本《鲁拜集》版本非常少见。那么这本书对他来说是宝贵的吗？既然萨默顿男子在这本书上写了字，看来他并没有努力让这本书保持完好。

这本特殊的《鲁拜集》之所以被选中，也许是因为它具备了以下3个特点：

1. 少见（《鲁拜集》虽不少见，但是这个版本非常少见）；

2. 常见（考虑到《鲁拜集》有许多不同的版本，《鲁拜集》总的来说是一本常见的书）；

3. 不容易引起他人的怀疑。

关于第3点，我必须提醒读者注意，《鲁拜集》是一本非宗教性质的书。如果持有这本书的人被怀疑是苏联间谍，那么在他的藏书中，这本《鲁拜集》并不会引起调查者的特别注意。而如果苏联间谍选择另一本既常见，又有许多不同版本的书——《圣经》作为密码用书，就很容易引起调查者的怀疑。调查者很容易想到，既然共产党分子应该是无神论者，那么他持有一本《圣经》就显得很不自然了。

上面列出的第1点和第2点看起来似乎是互相矛盾的，但其实这两点并不矛盾。同一本书的不同版本之间可以有很大的差异。比如，不同版本的《鲁拜集》中作者诗歌的排列顺序会完全不同，此外具体文字（译文）也会有差异。之所以会出现这样的变化，可能是因为《鲁拜集》这本书刚面世的时候并不受读者欢迎。因此《鲁拜集》每出一个新版本，译者菲茨杰拉德可能都会尽力做一些改动，以期获得读者的青睐。

许多研究者都把萨默顿男子密码当作一种基于书籍的密码，他们希望以《鲁拜集》为基础来破译这段密码。然而，由于这些研究者所持有的《鲁拜集》并不是该案中那个特定的版本，所以他们的努力都没能获得成功。

一位护士使案情更加扑朔迷离

因为写在《鲁拜集》上的这段密码有许多不同的解法，我们又没有办法判断究竟哪一种解法才是密码书写人的原意，所以案情似乎已经走进了死胡同。仅从密码破译的角度来看，以上的判断可能是正确的。然

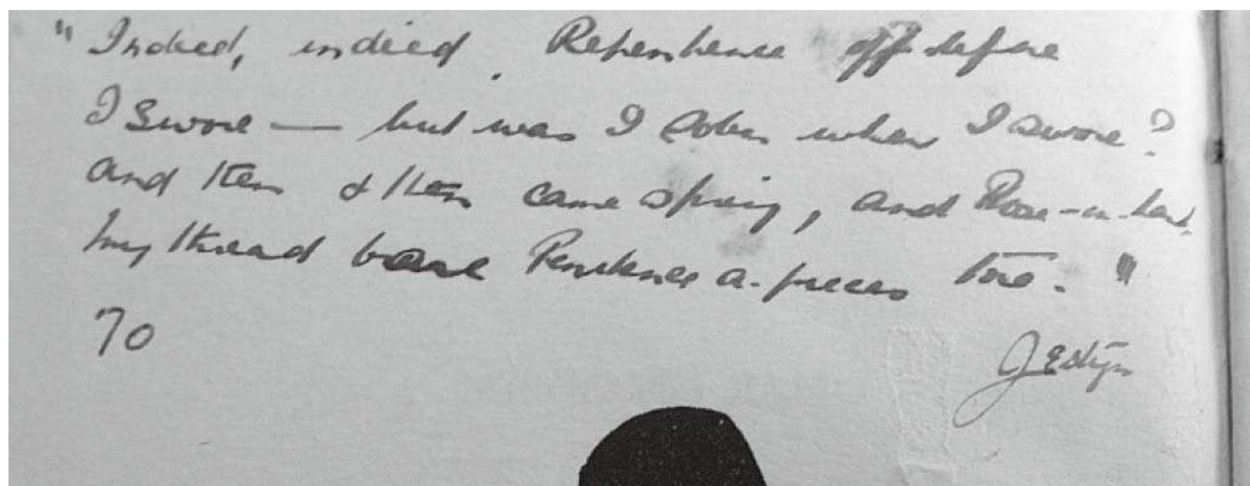
而，这本《鲁拜集》还为我们提供了性质截然不同的另一条线索——除了密码以外，这本《鲁拜集》中还有一个手写的电话号码。(注)

对于警方而言，查明一个电话号码属于谁是一件相当简单的工作。在萨默顿男子案中，许多人都使用了化名，然而这个电话号码的所属人的真名却非常清楚，这个女人的名字叫杰茜卡·哈克尼斯（Jessica Harkness）。许多文献仅以“护士”(注)二字称呼她。虽然费尔特斯成功地找到了她，并与她进行过交谈，但费尔特斯在书中以化名特雷莎·约翰逊（Teresa Johnson）来指代她，以保护这名证人及其家人的隐私。读者不久将会看到，杰茜卡的多位家庭成员已经主动向公众公开了自己的身份，因此现在已经没有必要继续用化名来称呼她了。事实是，萨默顿男子的尸体被发现的地点离杰茜卡的家只有1/4英里远。而且，杰茜卡家离《鲁拜集》被发现的地点也非常近。作为一名护士，杰茜卡是否了解并找到了一种法医无法检出的特殊毒药呢？警方显然也怀疑过这一点。出于某种原因，杰茜卡从一开始就对警方说了谎。比如，杰茜卡声称，她最近刚与一名叫普罗斯珀·约翰逊（Prosper Johnson）的人结婚。然而，这并不是事实。虽然后来杰茜卡确实与普罗斯珀·约翰逊结了婚，但在警方讯问杰茜卡的时候，二人并未结婚。普罗斯珀在认识杰茜卡之前就已经结婚，直到20世纪50年代初，普罗斯珀的离婚手续办妥之后，他才最终与杰茜卡成婚。至于这本《鲁拜集》上为什么会有杰茜卡的电话号码，杰茜卡自己的解释是，她将这本书送给了一个叫阿尔弗雷德·博克索尔（Alfred Boxall）的人。于是，我们就得到了一条令人兴奋的新线索——也许阿尔弗雷德·博克索尔就是我们要找的萨默顿男子！

阿尔弗雷德·博克索尔似乎是一个非常爱国的人。在第二次世界大战中，他虽然没有义务入伍，却主动选择参军，为澳大利亚而战。1942年1月12日，虽然博克索尔已经35岁，并且有妻子和孩子，但他仍然选择入伍。当时，只有年龄在19~33岁之间的男性才有义务参军。博克索尔的女儿莱斯莉是这对夫妇的第二个孩子，莱斯莉于1944年6月14日出生，而博克索尔则幸运地被调到了一个离家较近的职位上。他的工作地

点是悉尼港北岸的军事综合体，这里距离克利夫顿花园酒店很近。在克利夫顿花园酒店的酒吧里，一名与博克索尔共事的军官的女友将博克索尔介绍给了护士杰茜卡。博克索尔和杰茜卡认识的具体日期不详，但是我们知道，两人相处得很好，很有共同话题，包括博克索尔新出生的女儿，以及《鲁拜集》。

后来，两人在同一地点（克利夫顿花园酒店的酒吧）偶然再次相遇，杰茜卡赠给博克索尔一本题过字的《鲁拜集》（参见图6–13）。杰茜卡的署名是“杰斯廷”（Jestyn），但她的真名是杰茜卡·哈克尼斯。1945年6月，博克索尔被派往海外，此后他似乎再也没有见过杰茜卡。



"Indeed, indeed, Repentance oft before
I swore — but was I sober when I swore?
And then and then came Spring, and Rose-in-hand
My threadbare Penitence a-pieces tore."
70
Jestyn

图6-13 杰茜卡写在她送给阿尔弗雷德•博克索尔的《鲁拜集》上的题字

图中文字翻译如下：

真的，我从前也常常起誓改悔——

不过，起誓的时候我可曾酒醉？

待到春风一吹，我又手拈玫瑰——

那陈旧的忏悔已被撕得粉碎。(注)

杰斯廷

警方曾希望能确认萨默顿男人的身份就是阿尔弗雷德·博克索尔，然而这种希望很快就化为了泡影。警方获得了他并不是萨默顿男人的强有力的证据：博克索尔被找到了，而且他承认，杰茜卡确实曾经赠送过一本《鲁拜集》给他。而且更让警方崩溃的是，博克索尔表示，这本《鲁拜集》目前仍然在他手上！在被调往海外之前，博克索尔将这本《鲁拜集》转送给了他的妻子。据他回忆，他赠书给妻子的时间是1945年6月，而他的妻子认为赠书的时间是1944年圣诞节。经调查发现，博克索尔家里有两本同样的《鲁拜集》，因此也许他曾两次将同一本书的不同版本赠送给自己的妻子（在人类的历史上，还有许多其他丈夫也犯过同样的错误）。

博克索尔手上的《鲁拜集》与萨默顿男子的《鲁拜集》版本不同。[注]因此，假如真的有哪个间谍集团垄断了这个珍稀版本的《鲁拜集》，似乎博克索尔也并不是其中一员！

由于这本《鲁拜集》上的电话号码把杰茜卡拖入了萨默顿男子案，而杰茜卡又把博克索尔拖入，所以杰茜卡和博克索尔的个人生活变成了此案研究者们怀疑和猜测的主题。格林伍德认为，杰茜卡在这本《鲁拜集》上的题字是希望博克索尔与她展开或者保持婚外恋关系。然而，此后博克索尔却把这本书转赠给了自己的妻子。格林伍德认为这种情况“要么是极度的厚颜无耻，要么是极度的无知，要么就是出于一些更加奇怪的原因”。[注]博克索尔已经于1995年去世，因此我们已经没有办法再去询问他究竟为什么要把这本《鲁拜集》转赠给妻子了。然而，博克索尔似乎从未打算要隐瞒什么。在1978年的一次电视访谈中，他向公众展示了护士杰茜卡在《鲁拜集》上的题字。

由于博克索尔这条线索似乎走进了死胡同，所以警方自然又将关注重点转回到护士杰茜卡身上。我们知道，杰茜卡曾向警方说谎。此外，警方复原了萨默顿男子的行程，而杰茜卡似乎就是这次行程的重点，这就使杰茜卡告诉警方的故事变得更加可疑了。1949年的死因讨论会上详细讨论过萨默顿男子生前的行程，因此我们不妨从这次会议的记录材料

入手研究这段行程。克莱兰在这次讨论会的总结介绍中写道：

> 据警方认为，死者肯定是先乘火车来到阿德莱德火车站，将行李箱寄存在行李室中，接着购买了一张去亨利海滩的火车票，却没有赶上这趟火车。于是死者改搭公共汽车来到萨默顿海滩。阿德莱德火车站行李室的接待员、售出这张去亨利海滩的火车票的售票员，以及开往萨默顿沙滩的公共汽车上的售票员都不记得曾经看到死者。从这辆公共汽车到达萨默顿海滩的时候到当天晚上7点钟，也没有任何目击证人看到死者。㊟

阿德莱德火车站衣帽间的高级管理员哈罗德·罗尔夫·诺思（Harold Rolfe North）给出了以下证词："在阿德莱德火车站中，目前没有供旅客洗澡和剃须的地方。"㊟因此，萨默顿男子可能是为了在上火车之前洗个澡而去了城内的浴室，这使他没能赶上开往亨利海滩的火车。然而，还有其他一些线索需要考虑：

> 当时，公众强烈要求将亨利海滩的铁路线延长到格莱内尔格。一些未经证实的报告称，1948年时，在阿德莱德火车站里挂有一些地图，上面画出了尚未开通的从亨利海滩开往格莱内尔格的铁路线。㊟

如果这些报告内容属实的话，我们就又有了一种新的可能的解释。这名身份不明的男子之所以购买前往亨利海滩的火车票，也许是因为他以为这趟车能带他去往他的目的地。后来，男子发现这趟车并不能到达他想去的地方，因此决定改搭开往萨默顿海滩的公共汽车。

在萨默顿男子持有的这本《鲁拜集》上，写有住在阿德莱德的护士杰茜卡的电话号码。因此，费尔特斯认为萨默顿男子应该曾经给杰茜卡致电，却没有人接。我还没找到任何原始文件来证明萨默顿男子曾经打

过电话，只有报纸上的一些文章中提到了这一点。事实上，就算萨默顿男子曾经打过电话，当时的技术也未必能够证实这一点。如果萨默顿男子确实打过电话，他应该使用的是公用电话，然而从警方的记录来看，警方似乎从来没有调查过萨默顿男子可能使用过的公用电话的通话记录。

故事可能是这么发展的：萨默顿男子不仅打过电话，还到过护士杰茜卡家，并且敲了门，然而没有人应答。杰茜卡的一位邻居告诉萨默顿男子，杰茜卡和她的孩子都不在家。据称，听到这个答案以后，萨默顿男子露出了惊讶的表情。然而，我们如何能确定这个故事的真实性呢？媒体对此案的报道充满了各种错误、矛盾，并且常常把猜测当作事实来写。如果警方关于此案的文件还没有丢失的话，我们或许能够确认这些证据是否属实。

如果我们只关注本案中各处关键地点之间的距离，用一份现代地图也足够了。这几处地点之间的距离关系如图6–14所示。



图6-14 该地图上标示了本案的若干关键地点

A. 阿德莱德火车站

B. 格莱内尔格莫斯利街，护士杰茜卡•哈克尼斯居住的地方

C. 萨默顿公园海滩

D. 萨默顿男子被埋葬的地点：西街墓地，地址是西街161号

此时，警方已经放弃了萨默顿男子的身份就是阿尔弗雷德·博克索

尔的猜想。而且，警方也都知道了我在上几段中提到的这些信息。他们又回去找护士杰茜卡，并询问她能否指认死者的身份。据描述，杰茜卡的反应是“大吃一惊，差点儿就要晕倒了”。[注]然而，杰茜卡却声称她无法确认死者的身份。

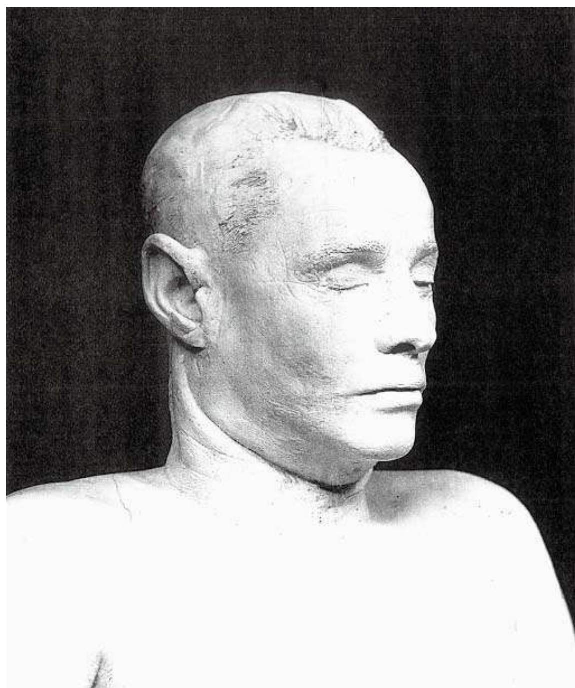


图6-15 这名身份不明的男子的半身像——看这幅图你会晕倒吗？

如果杰茜卡真的不认识死者，那么为什么她在看到死者的形象时会惊讶得差点儿晕倒呢？我们无法判断当一个人第一次看到尸体时到底会受到多大的惊吓，但是作为一名护士似乎应该已经习惯了这种场景。而且，杰茜卡看到的场景事实上并没有那么阴森恐怖——警方让她看的并不是萨默顿男子的尸体，因为当时萨默顿男子的尸体已经被埋葬了，杰茜卡看到的只是萨默顿男子的半身像而已。

格里·费尔特斯通过《鲁拜集》上的电话号码以及一本阿德莱德市的老电话号码簿找到了护士杰茜卡。2002年，费尔特斯与杰茜卡见面进行了一次长谈。费尔特斯在书中回忆道：“她不断地将话题从萨默顿男子案上转移到别处。”[注]通过这次对杰茜卡的访谈，费尔特斯愈加确信：杰茜卡其实知道萨默顿男子的身份。

虽然杰茜卡向警方诉说的故事非常可疑，但她却一直坚持自己的说辞。也许，杰茜卡和这位身份不明的男子之间有一段令她尴尬的故事。人们曾经希望，在杰茜卡的丈夫死后，也许她会愿意透露更多关于萨默顿男子的信息。然而，即使在杰茜卡的丈夫去世以后，她依然对此事保持沉默。也许，她害怕的不是丈夫的指责，而是公众的指责。

五只眼睛组织和间谍

今天，有一个叫作“五只眼睛”（Five Eyes）的情报组织，其成员国包括美国、英国、加拿大、澳大利亚，以及新西兰，各成员国之间会共享情报信息。“五只眼睛”组织是由第二次世界大战时期美国和英国之间的一个合作组织演化而来的。当时，美英两国的分工是：美国主要负责破译日本的密码和暗号，而英国主要负责破译德国的密码和暗号。这种分工方式能够让美英两国更高效地破译敌方的密码。在此后的这些年中，美英两国之间的这种合作关系不断加强，并且其他国家也相继加入了这个组织。现在，“五只眼睛”组织还包括一些级别较低的成员国，这些成员国可以获得组织内的部分情报。然而，在加入这个精英俱乐部以后，澳大利亚却出师不利。

1947年4月，美国陆军安全局的密码专家梅瑞迪思·加德纳（Meredith Gardner）发现，苏联情报总部和澳大利亚堪培拉苏联大使馆的某些情报在加密的时候反复使用了同一个一次性密码本。在《未解之谜（下）》的第8章中我们将会谈到，这会让加密的信息变得容易破译。同年5月，美国陆军安全局请求英国情报破译组织——政府通信总部与他们合作破译这些密码。这次行动中破获的情报代号为“薇诺娜”（Venona）。到1947年11月25日，英美两国破译的信息显示，从1945年开始，就有一些机密的英国情报被泄露给了苏联方面，而泄露情报的机构很可能是澳大利亚外交部。

由于这次不愉快的事件，1948年，美国决定停止与澳大利亚共享加密信息。因为此事的发生，澳大利亚政府决定以更加严肃的态度来开展反间谍活动。[注]

令澳大利亚政府深感为难的是，代号为“薇诺娜”的这些情报没有办法作为证据在法庭上出示，因此，有些间谍虽然身份已经被发现，却逃过了澳大利亚政府的起诉。当然，即使没有被送上法庭，这些间谍的职业生涯也已经宣告结束了。由于这些已被发现的间谍人员也可能反过来

泄露苏联方面的情报，所以苏联政府对这些人十分紧张。但是，苏联政府是否已经紧张到了要杀掉他们的程度呢？

读者可能还记得，在1949年对萨默顿男子的死因讨论会上，有一名专家证人曾提出致死毒药可能是洋地黄苷。在维基百科的“Tamam Shud案”词条下，该词条的作者试图通过两条来源建立一种阴谋论。其中的第一个来源进一步证实了毒药是洋地黄苷的假说。

> 1994年，维多利亚省首席法官兼维多利亚法医学研究所主席约翰·哈伯·菲利普斯（John Harber Phillips）重新审阅了萨默顿男子案的卷宗，以期找出萨默顿男子的死因。他的结论是：“死因是洋地黄苷，关于这一点似乎没有太多疑问。”(注)

在同一篇文章中，与上一段内容仅隔了一句话后又出现了这样的内容：

> 在这名身份不明的男子死前3个月，即1948年8月16日，有报道称美国助理财政部部长哈里·德克斯特·怀特（Harry Dexter White）死于过量的洋地黄苷。此前，根据薇诺娜情报，他曾被控泄密给苏联方面。(注)

在维基百科的这个词条中，作者列出的以上一段文字的出处是：Willard Edwards, “Hiss spy paper linked to late treasury aid [sic]，” (*Chicago Daily Tribune*, November 29, 1949): 1–2。然而，在威拉德·爱德华兹撰写的这篇文章中，只对怀特的死做了如下的描述：“当时，他声称自己的心脏有些小毛病。不到一个星期，在8月17日这一天，他死在自己家中。据报道称，他的死因是过量使用洋地黄苷。”这篇文章中并没有具体写出所谓的“据报道”究竟是谁的报道，因此这条线索也走进了死胡同。而另一位研究者则发现，只要稍做调查就可以发现上述说法事

实上是没有根据的。

> 关于他的死，出现了许多神秘的谣言，但是在《波士顿环球报》（Boston Globe）的一次采访中，乔治·S.埃默森（George S.Emerson）医生为我们驱散了这些疑云。这次访谈中展示了怀特的死亡证明的复印件。从死亡证明上来看，医生认为死因是“由心脏冠状动脉病变引起的冠心病发作”。以下这本书也确认了怀特的死因确实是冠心病发作，即戴维·里斯（David Rees）所著的《哈里·德克斯特·怀特：悖论的研究》（Harry Dexter White: A Study in Paradox），此书1973年由科沃德、麦卡恩和盖根出版社出版。[注]

除了维基百科以外，以下这个网址中也引用了同一个出处：http://www.globalresearch.ca/us-intelligence-and-the-fate-of-the-private-pre-war-international-banking-system/5378602?print=1。然而，该网页的引用部分还加了以下内容：

> 签发怀特死亡证明的医生（怀特死时这名医生并不在场）事后否认怀特死于洋地黄苷。最近，一名右翼作家约翰·科斯特尔（John Koster）称，怀特是为了自杀而服用了过量的洋地黄苷，他的唯一证据是一部怀特可能看过的当代电影。（来源：John P.Koster, Operation Snow: How a Soviet Mole in FDR’s White House Triggered Pearl Harbor Washington: Regnery Publishing, 2012, 204－05）.

综合考虑以上信息，我认为怀特并非死于过量的洋地黄苷。毕竟这种理论的证据只是威拉德·爱德华兹发表在《芝加哥每日论坛报》（*Chicago Daily Tribune*）上的一篇报道。假如《芝加哥每日论坛报》能信的话，杜威就是总统了。[注][注]

虽然我们可以通过调查证实某些谣言其实是没有根据的，但是萨默顿男子是一名间谍的理论却很难被彻底排除掉。比如，即使我们检查过所有已经解密的薇诺娜文件都找不到任何与萨默顿男子有关的内容，也并不能证明萨默顿男人肯定与间谍活动无关。因为即便薇诺娜计划破获了大量苏联情报，“五只眼睛”组织也不可能找出潜伏在澳大利亚的所有苏联间谍。1954年，当时正在澳大利亚工作的克格勃间谍弗拉基米尔·彼得罗夫（Vladimir Petrov）招供出了更多潜伏在澳大利亚的苏联间谍。澳大利亚的情报机关以最为容易的方法抓到了彼得罗夫——他自己叛变了苏联。而且，在薇诺娜情报中，通常只包含苏联间谍的代号，要把这些代号和间谍的真名匹配起来又是一项艰巨的工作。在薇诺娜情报提供的间谍代号中，有大约一半的代号最终并没能与现实中的间谍联系起来，因为情报部门一直找不到代号背后的真实身份。

那么，这么多苏联间谍究竟在澳大利亚做什么呢？有两件事情是苏联间谍特别感兴趣的：

1. 1944年，南澳大利亚发现了铀矿。当时，除了澳大利亚以外，只有以下几个国家发现过铀矿，这几个国家是：加拿大、捷克斯洛伐克和比属刚果。

2. 1946年11月，澳大利亚宣布，他们正在南澳大利亚地区建设一个名为“乌美拉”（Woomera）的火箭试射基地，而离该试射基地最近的大城市就是阿德莱德。20世纪50年代，乌美拉基地曾进行过英国—澳大利亚两国联合核试验。萨默顿男子密码中的第一个字母W是否就代表乌美拉基地呢？

关于萨默顿男子身上的那张未使用的火车票，各路研究者提出了若干种假设。如果我们接受萨默顿男子与间谍活动有关的理论，那么关于这张火车票的假说就又多了一种。

也许，萨默顿男子发现自己被某人跟踪，或者某个他害怕的人也正

要登上同一列火车，因此，萨默顿男子在火车发车前逃离了开往亨利海滩的火车，试图躲开敌人。此外，我们也可以认为萨默顿男子是故意将自己的《鲁拜集》丢掉的。之所以必须丢掉这本书，可能是因为这本《鲁拜集》中包含着密码或者电话号码，也可能是因为其他一些原因，总之这本书可能是萨默顿男子不希望被敌人发现的敏感物件。但是，如果要丢掉这本书的话，丢在垃圾桶里不是更合理吗？为什么要把这本书丢在一辆车里呢？也许，当时的情况使得萨默顿男子必须快速丢掉手中的《鲁拜集》，而附近却又正好找不到垃圾桶。

军火走私商？

萨默顿男子来澳大利亚的目的是什么？关于这个问题，格林伍德在自己的非虚构类著作里提出了两种猜测。作为第一种猜测，她引用了自己写的一部（虚构的）短篇侦探小说，属于芙里尼·费希尔（Phryne Fisher）侦探系列。在这篇侦探小说中，萨默顿男子参与了向爱尔兰走私军火的活动。而第二种猜测则是这本书的原创，在这种猜测中，萨默顿男人仍然是军火走私人员，只不过走私的目的地变成了以色列。在第二种猜测中，格林伍德认为萨默顿男子的真名是雷诺兹（Reynolds），我们会在稍后的篇幅中谈到这个名字的出处。格林伍德的这两种说法都没有什么证据支持，但是也没有明确的证据能完全排除这两种可能性。格林伍德列出的证据包括：萨默顿男子手腕上的“鲸鱼痕”伤疤（前文提过）、萨默顿男子的所谓“货船装卸指挥员”工具，以及其他一些并不太有说服力的琐碎花边新闻。

即使萨默顿男子真的向以色列走私军火，他也不太可能是犹太人。死因讨论会的记录上明确写了萨默顿男子没有受过割礼。然而在萨默顿男子死后，似乎有些犹太人对他表示了敬意。萨默顿男子的坟墓上堆着一些卵石，这是传统的犹太丧葬习俗。传统犹太习俗并未规定只能在犹太人的墓上放这种卵石，也许献这些卵石的人只是想感谢这位异教徒帮

助他们武装以色列。有些读者可能记得，在斯皮尔伯格的电影《辛德勒的名单》的末尾，奥斯卡·辛德勒的墓上也摆着犹太人献上的卵石。当然，辛德勒受犹太人感谢的原因与走私军火并无关系。

萨默顿男子的私生子

在前文中，我曾提过这名身份不明的男子“身上还有其他一些奇怪的特征”。这些奇怪的特征使得他和护士杰茜卡的联系又多了一处。请读者看下面的图6–16。乍一看，图中画的只是两只耳朵而已。但是如果仔细观察的话，左边的耳朵（萨默顿男子的耳朵）和右边的耳朵其实又有一些不同。左图的这只耳朵耳甲艇比耳甲腔大，而绝大部分人的耳朵是右图的这种——也就是耳甲艇比耳甲腔小。护士杰茜卡的耳朵是右图这种常见的耳朵。

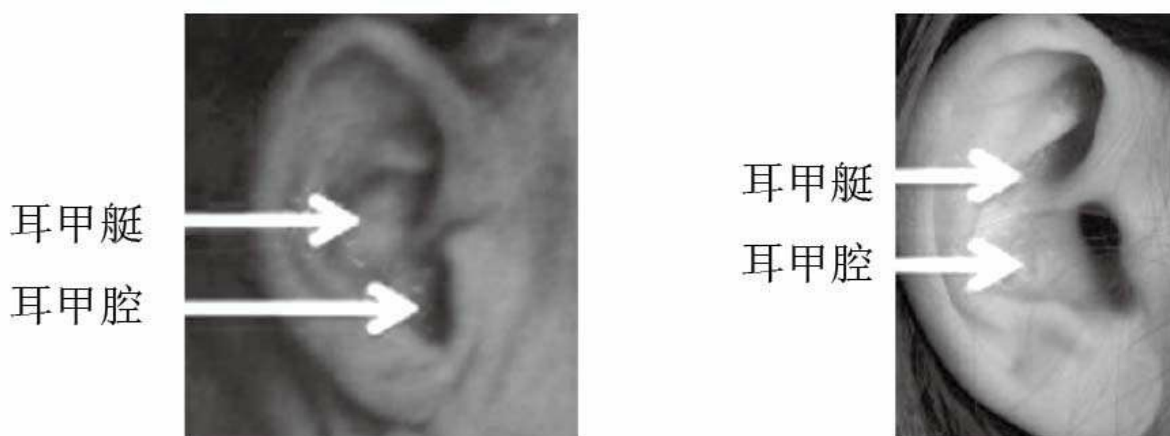


图6-16 萨默顿男子的耳朵（左图）与更常见的耳朵（右图）的对比

那么，萨默顿男子的耳朵是如何把他和护士杰茜卡联系起来的呢？虽然杰茜卡的耳朵是右图这种常见的耳朵，但她的儿子罗宾（Robin）的耳朵却是左图这种比较罕见的耳朵。

此外，罗宾和萨默顿男子还具有一种共同的基因缺陷——双侧侧切牙过多（这种基因缺陷的症状是牙齿数目比正常人多）。在人群中，只有2%的人有牙齿过多的基因缺陷，而图6–16中左图的耳形出现在人群

中的概率甚至更低，只有1%~2%的白人的耳朵是左图的形状。

根据上述线索，我们很容易联想到萨默顿男子可能是罗宾的生父，因此护士杰茜卡声称自己完全不认识死者的说法就显得更不可信了。

阿德莱德大学的德里克·阿博特教授估计，因为萨默顿男子与罗宾同时拥有上述两种罕见的特征，萨默顿男子和罗宾完全没有亲戚关系的概率在1/10 000 000~1/20 000 000之间。而在格林伍德的书中则直接采用了1/20 000 000这个更低的数字。

然而，在计算某一概率的时候，只要多考虑或者少考虑几个因素，就可以拉低或者拉高概率的计算结果。为了举例说明这个问题，让我们来分别考虑牙齿过多的概率（2%），以及上述特殊耳形出现的概率（1%）。由于一个人有这种特殊耳形的概率事实上在1%~2%之间，所以我们在计算概率的时候也可以取2%作为出现这种特殊耳形的概率，或者我们可以折中一下取这个范围的中间值，也就是1.5%。我们在这里取的数值越小，最后所得到的概率估计也就越低。但是，不管对特殊耳形的概率取多大的值，计算最终概率的方式都是一样的：先将百分数转化为小数，然后再把这两个概率相乘。将上述概率代入公式，我们得到：$0.02 \times 0.01=0.000\ 2$。也就是说，同时拥有这两种特征的概率是1/5 000。这个结果比上一段中德里克·阿博特教授的估计值要大了许多！接下来，如果我们还想引入更多因素，我们可以考虑萨默顿男子和罗宾都是白人的事实。如果两个人中有一个是埃塞俄比亚人，另一个是纯种彻罗基印第安人，那么我们几乎很难想象这两个人会有亲属关系。在全球的人口中，究竟有多大比例的人是白人呢？这就是一个我们可以引入的新因素。当然，如果我们希望得到非常严格的结果，我们应该使用南澳大利亚地区的白人比例，而不是整个世界人口中的白人比例，但这又是我们在计算过程中可以灵活操作的一个地方。另外一个可以考虑的因素是，我们知道萨默顿男子有护士杰茜卡的电话号码。在拥有你的电话号码的人中，有百分之多少与你没有血缘关系？上述问题的概率很难估计，这个问题的答案显然取决于你重视隐私的程度。我没有仔细研究过

阿博特教授究竟是如何得到上一段中的估计值（1/10 000 000到1/20 000 000之间）的，因为我认为不管这个概率有多小，都不能确定地证明萨默顿男子就是罗宾的父亲。反过来说，我认为即使是1/5 000这种较高的概率也足以让我们怀疑萨默顿男子与罗宾是存在亲属关系的。

如果我们认为萨默顿男子与罗宾有某种血缘关系，那么考虑到萨默顿男子的年龄和罗宾的年龄，最容易得到的结论是：这两人是父子关系。然而，这并不是唯一的可能性！在格林伍德的书中，她认为萨默顿男子是罗宾的叔叔或者其他血缘关系较近的亲属。在格林伍德的故事中，萨默顿男子是一名向以色列走私军火的贩子，护士杰茜卡可能是萨默顿男子的姐妹、侄女，或者表亲，因此萨默顿男子才想要去杰茜卡家拜访她。虽然杰茜卡与萨默顿男子有血缘关系，但萨默顿男子身上的两处不寻常的特征（即特殊耳形和牙齿过多）可能恰好没有表现在杰茜卡身上。

萨默顿男子案之所以能成为一桩经典的谜案，是因为此案具有所有伟大谜案的共同特征：对几乎每一条证据都可以进行多种不同的解读。你对这些证据又有什么看法呢？

类似的死亡事件

如果读者想要对萨默顿男子案建立更大的阴谋论，这里还有一些素材。第一则素材是1945年8月25日登载在报纸上的一篇报道（见图6–17）。(注)

在格林伍德所著的关于萨默顿男子案的书中也提到了这个案件。格林伍德认为，此事与萨默顿男子案没有任何关系。但她也为感兴趣的读者提供了其他一些信息。

此外，格林伍德还在书中提到了另一起与萨默顿男子案类似的事件。该事件发生于1881年，相关报道刊登在《南澳大利亚记录报》

（*South Australian Register*）上。1881年1月6日，有人看见一名衣着厚重的男子在沙滩上行走。同年1月10日，这名男子的尸体在沙滩上被发现。警方从未确认这名男子的身份，虽然男子身上有一把带血的剃刀以及另一把刀，但是验尸官认为："要想用这些刀具造成死者喉部的伤口是极不方便的。"验尸官认为此案很可能是一起自杀事件，但他给出的官方结论是"死因存疑"。(注)显然，这起发生于1881年的旧案与萨默顿男子案具有一些相似之处，但是此案中并没有出现《鲁拜集》。

珀斯一名诗人自杀，诗人以欧玛尔的诗作为他的墓志铭

6月3日，生活在珀斯的30岁男子约瑟夫·海姆·索尔·马歇尔（Joseph Haim Saul Marshall），昵称乔治（George），在悉尼泰勒湾海岸线附近的树丛中服毒自杀。他的死因讨论会于上周结束。约瑟夫的兄弟塞缪尔·索尔·马歇尔（Samuel Saul Marshall）之前生活在新加坡，目前已经移居珀斯。最近，塞缪尔向我们提供了一些惊人的证据。

约瑟夫·马歇尔自杀身亡时，胸前放着一本波斯诗人欧玛尔·海亚姆的诗集《鲁拜集》。死者用铅笔在诗集中标出了以下的诗句：

啊，把剩下的一切尽情地享用——

趁我们还没沉沦于泥土之中；

尘土复归于尘土，长眠尘土下——

无酒无歌无歌手，而且还无穷。(注)

死者的兄弟表示，约瑟夫7岁时曾在新加坡出过事故。此次事故影响了他的健康，也使他变得不喜欢参加社会生活。约瑟夫在18岁的时候被父母送往法国接受高等教育。在法国待了5年之后，约瑟夫"对于生活的态度似乎变得非常奇怪"。

约瑟夫的兄弟告诉我们："约瑟夫曾出版过一本诗集，题目是《只有你和我》。但是诗集出版以后获得的评价并不高，此事令约瑟夫感到极为沮丧。作为他的家庭成员，我们都非常爱约瑟夫，约瑟夫也非常爱我们。1929年，父亲损失了许多财产，乔治在我们所有人都不知情的情况下，为自己购买了巨额的交通事故人寿保险。在保险合同满一年的时候，乔治打算开着车驶下悬崖，这样我们就能获得巨额保险金了。好在我们及时发现了他的自杀企图。"

约瑟夫·马歇尔于1939年来到澳大利亚，他在澳大利亚过着隐居的生活，喜欢读有哲学倾向的书。后来约瑟夫在物价调控委员会工作过。

图6-17 一篇报道了另一宗与萨默顿男子案类似的离奇死亡事件的报纸文章

访问班伯里

他的兄弟说："在一封写给他朋友的信中，约瑟夫将物价调控委员会描述得非常可怕，他说物价调控委员会'快要变成一个疯人院了，而他则要为此付出代价'。这一年的1月1日，约瑟夫被关进了希思科特(注)，因为有三名医生都签发了他精神失常的证明。而在此事发生之前，约瑟夫刚刚访问过班伯里。"

"在班伯里，约瑟夫过量服下了某种药物。但是药物却没有起效，约瑟夫在服药以后走到了海水边缘，在那里被警察逮捕。接着，医生对约瑟夫注射了大量胰岛素。最后，医生别无选择：要么把约瑟夫关进精神病院，要么约瑟夫必然会找机会让自己变得更加稳定。"(注)

"我毫不怀疑，约瑟夫的死法是他自己选择的，那是他认为最好、最高贵的结束生命的方式。我个人认为，约瑟夫死时身边放着的那瓶水应该是用作某种净化仪式。"

新南威尔士州罗克代尔的一名理发师格温妮丝·多萝西·格雷厄姆（Gwenneth Dorothy Graham）表示，4年来她一直与约瑟夫保持着十分友好的关系。她最后一次见到约瑟夫·马歇尔是在5月19日，那天他们一起吃了晚餐。

格雷厄姆补充道："约瑟夫常常建议我自己开一个发廊，他说开设发廊的花费大概是2 000澳大利亚镑。听到他的话我笑了，我说：'不，大概是200澳大利亚镑。'5月19日，约瑟夫告诉我，他给我寄了一张200澳大利亚镑的支票。我在第二周的星期一收到了这张支票。"

验尸官库克森（Cookson）发现，约瑟夫·马歇尔死于一种巴比妥酸化合物中毒，这种毒药是他自愿服下的。

图6-18 这篇新闻报道的结尾

也就是说，在1881年、1945年和1948年，沙滩上共发生了三起疑似自杀或谋杀的案件。如果这种事情是发生在《X档案》中的话，这3起案件之间的时间间隔可能会正好相等，然而事实却不是这样。此外，我们必须正视一个悲伤的事实，那就是：自杀事实上是一种相当常见的现象。每年都会发生大量的自杀事件，所以其中某些自杀事件与萨默顿男子之死具有一些共通之处事实上是完全合理的。

欢迎来到奇幻世界

有一个网站讨论了关于萨默顿男子案的三种假说。第一种是间谍说（该网站认为间谍说的可信度有4分，满分为5分），而另外两种假说则比间谍说还要奇幻。我将该网站的另外两种假说抄录如下，并附上该网站对这两种假说可信度的评分。(注)

1.萨默顿男子是一名时间旅行者

这是一种比较奇幻的理论。在案件发生后的这些年中，有些人一直认为萨默顿男子是一名时间旅行者。这种理论能够解释为什么萨默顿男子的衣服上没有名牌，也能够解释为什么任何人都确定不了他的身份，因为他来自另一个时代。这种理论甚至也可以解释萨默顿男子的脚的奇怪形状。也许，在他所处的时代，尖头鞋是一种非常流行的款式。萨默顿男子身上之所以会有一些奇怪的工具，是因为他需要用这些工具来维护他的时光机。《鲁拜集》的密码是不是他回程必须用到的某种密码呢？

此外，还有人提出，“杰斯廷”可能与萨默顿男子有某种亲戚关系（比如她可能是萨默顿男子的曾祖母）。因此，杰斯廷才不愿透露更多自己的信息。

不幸的是，没有任何证据能够证明萨默顿男子是一名时间旅行者。此外还有一个问题是，时间旅行也许根本就是不可能的。

Weirld.com[注] 可信度评分：1/5

2. 萨默顿男子是基因改造人，或人类和外星人的混血物种，或基因实验的产物

萨默顿男子牙齿有缺陷、耳甲艇较大、小腿肌肉发达，这些都是不寻常的基因特点。从验尸之后拍摄的照片中，似乎还可以看出萨默顿男子的脸部特征也有一些不同寻常的地方。因此，有人提出萨默顿男子可能是某种基因改造人，或者他可能根本不是人类——比如是人类和外星人的混血物种。这种理论能够解释萨默顿男子生理上的这些异常之处。

然而，虽然牙齿缺陷的症状可能与某些先天疾病或综合征有关，但是在总体人群中也大约有2%的人会出现这种症状。耳甲艇较大的性状在普通人群中也同样有一定的概率出现。而造成小腿肌肉

发达的原因则有很多，比如，可能此人体格特别健壮。

在不进行基因检测的情况下，我们无法排除萨默顿男子是基因改造人的可能性，但这种情况看起来概率很低。萨默顿男子的脸部特征之所以在照片中看起来有些奇怪，可能仅仅是因为在验尸后他的容貌因为尸体肿胀而发生了一些变化，此外对尸体进行的防腐措施也有可能改变一个人的容貌。

Weirld.com可信度评分：1/5

格林伍德在她的书中简要提到了上述两种理论。在这里我必须要为格林伍德正名：对于这两种理论的可信度，她也给予了极低的评分。

身份不明的男子

在犯罪史上不乏这样的例子：在某位作者的畅销书使陈年旧案重新获得公众关注以后，这些旧案可能会出现一些全新的线索。在“BTK杀手”一案中，罗伯特·贝蒂（Robert Beattie）功不可没。由于贝蒂写的一本书，BTK杀手案在尘封几十年以后，不仅找到了凶手，警方甚至还靠充分的证据将凶手逮捕和定罪。罗伯特·格雷史密斯写了两本关于黄道十二宫杀手的书籍，其中一本书还被改编成了电影。虽然这两本书和一部电影都没有能够帮助警方找到黄道十二宫杀手的真实身份，但在它们面世以后，黄道十二宫杀手案也突然产生了许多新的线索。在此前的第5章中，我曾经提过一档名为《美国头号通缉犯》的节目。由于该节目的观众群巨大，这些观众根据节目中播出的内容为警方提供了大量破案线索。在该节目播出1 000多集之后，2008年5月2日该节目的官网宣布，他们已经成功帮助警方抓获了第1 000名通缉犯。(注)

除了《美国头号通缉犯》以外，还有另外一个节目也声称起到了类似的效果：

《悬案》（Unsolved Mysteries）节目在播出260期以来已经向观众展示了超过1 000起案件。在这1 000起案件中，有一半以上涉及在逃犯的案件后被警方侦破，其中大部分都是因为本节目观众提供的线索得以破获。此外，本节目中的“失去的爱”环节已经帮助超过100个家庭重新团圆，还有若干与继承人失踪、谋杀、诈骗以及失忆等情况有关的案件因为本节目的播出而被侦破。在7起案件中，此前被错误定罪的无辜人员因为《悬案》节目的播出而重获清白。㊟

因为萨默顿男子案是阿德莱德发生的一起著名案件，所以媒体一直关注着萨默顿男子案。然而，在退休警探格里·费尔特斯关于此案的书《身份不明的男子》（*The Unknown Man*）面世以后，媒体对此案的关注程度又有所攀升。在上述著作面世以后，一名不愿公布姓名的阿德莱德女子向警方提供了一张身份证，这张身份证是在她父亲的物品中发现的。下图中的这张身份证上的男子是否就是1948年死于萨默顿海滩上的无名男子呢？


Form 685
U. S. DEPARTMENT OF LABOR
IMMIGRATION SERVICE
SEAMAN'S IDENTIFICATION CARD
ORIGINAL
No. 58757
Name H C Reynolds
Age 18 on ...., 191
(Date)
Nationality British
Marks:
(Issued under Rule 10, Immigration Regulations.)
14—1279

图6-19 萨默顿男子的真实身份?

图6–19中展示的这张身份证是一张海员身份证明卡。这张卡是1918年在美国签发的，它的主人是一名18岁的英国公民，姓名为H.C.雷诺兹（H.C.Reynolds）。如果此人在1918年时年龄是18岁的话，那么在萨默顿男子尸体被发现的1948年，此人就应该是48岁，这与萨默顿男子的估计年龄十分吻合。此外，这张身份证照片上的男子也具有特殊的耳朵形状，以及一颗痣——这两点都与萨默顿男子的外貌特征高度吻合。[注]

2011年10月，这名不愿透露姓名的女士将她找到的这张身份证交给了马切伊·亨内贝格（Maciej Henneberg）教授。亨内贝格教授是生物人类学专家，并且是身份鉴定方面的著名专家。他的鉴定结论是：“由于照片上男子的耳朵特征以及痣的位置都与萨默顿男子高度相似，我可以明确判断此人就是萨默顿男子。从法医学的角度，我们极少能做出这种明确的判断。”

这名不愿透露姓名的女士还联系了澳大利亚的《星期日邮报》（*Sunday Mail*）。《星期日邮报》按照这张身份证上的信息查找了美国国家档案馆、英国国家档案馆，以及澳大利亚战争纪念研究中心的档案，然而都没有找到关于该男子的记录。如果雷诺兹与这名不愿透露姓名的女士的父亲没有亲属关系的话，我们就不得不提出这样一个问题：为什么这位女士的父亲会持有雷诺兹的身份证呢？这位女士的父亲是否从萨默顿男子的尸体上取走了这张身份证，并作为战利品保留了下来？

在本书的第1章中，我们曾提到尼克·佩林对伏尼契手稿做的工作。佩林对雷诺兹的生平也进行了研究（他的研究似乎比《星期日邮报》的研究更成功一些），根据这些研究的结果，他认为萨默顿男子的身份不太可能是雷诺兹。

更多线索

然而，关于萨默顿男子案的线索还在不断地涌现出来，并且这其中有一些可以说非常出人意料。布朗警探认为，在相关人员的家庭成员去世以后，也许会有更多关于萨默顿男子的信息浮出水面。然而，我在前文中已经说过，这一希望后来也落空了。1995年，杰茜卡的丈夫去世，但杰茜卡仍然选择保持沉默，因此萨默顿男子案最终告破的希望变得更加渺茫了。2007年，杰茜卡本人也去世了。我想，不论是谁也能判断出，随着杰茜卡的离世，揭开本案真相的概率又下降了。然而，若干年以后，又出现了一条萨默顿男子案的新线索。这条线索几乎可以说是一段来自坟墓的口供。

2013年11月，护士杰茜卡的女儿凯特·托马斯（Kate Thomas）声称，母亲生前曾向她承认自己对警方说了谎，并承认自己其实知道萨默顿男子的真实身份。凯特是在接受澳大利亚版的《60分钟》节目的采访时发表上述声明的。[注]不过杰茜卡并没有告诉女儿萨默顿男子的真实姓名，她只说："这是一个秘密。只有比警方更高层的机构才知道。"

该节目的解说员将护士杰茜卡描述为一个“同情共产主义”的人，而凯特则确认她认为自己的母亲是一名间谍。据凯特回忆，杰茜卡曾在与几位苏联移民见面后说自己还能听懂俄语。当凯特很自然地问母亲是在哪里学的俄语时，杰茜卡却没有回答。在这次访谈中，凯特并没有流露出太多对母亲的爱。相反，她说：“她有阴暗的一面，非常黑暗的阴暗面。”凯特甚至还表示：“我一直有一种恐惧，我想也许母亲要对他（指萨默顿男子）的死亡负责。”

凯特认为萨默顿男子也是一名间谍，并且她的母亲和萨默顿男子有过恋爱关系。虽然凯特的父亲是普罗斯珀·约翰逊，但是杰茜卡此前曾以单身母亲的身份带着另一个孩子生活——这个孩子就是凯特的哥哥罗宾。罗宾生于1947年7月，在萨默顿男子死亡的时候，罗宾的年龄是1岁4个月。

《60分钟》节目甚至还找出了其他可能与萨默顿男子有亲属关系的人。罗马·伊根（Roma Egan）是罗宾的妻子，她也认为丈夫罗宾的生父其实就是萨默顿男子。伊根的证据是罗宾和萨默顿男子有两处相似的生理特征，这项证据我们在前文中已经说过了——罗宾和萨默顿男子都具有一种少见的耳朵形状，并且牙齿都存在同样的不正常症状。如果伊根的猜测属实，那么她和罗宾的女儿雷切尔就应该是萨默顿男子的孙女。雷切尔和罗马·伊根都想知道事情的真相，她们愿意挖出萨默顿男子的尸体进行DNA（脱氧核糖核酸）测试。

然而要进行DNA测试还面临一重额外的困难，那就是萨默顿男子的尸体曾经用福尔马林做过防腐处理。[注]事实上，萨默顿男子的尸体是南澳大利亚地区首例采用这种新技术进行防腐处理的尸体。如果尸体被福尔马林处理过，进行DNA测试就会变得很困难。要提取有效的DNA，最好从死者的牙齿、骨骼，或者头发中提取，而从腐烂的软组织中提取的DNA则相对不适合DNA测试。

DNA测试可以告诉我们雷切尔是不是萨默顿男子的后代。此外，如果能把萨默顿男子的DNA与世界各地数据库中的DNA样本进行比较，

还可以判断出萨默顿男子来自世界上的哪个地区。然而即使进行DNA测试，也无法确定萨默顿男子的姓名，因为并没有疑似人的样本可供比较。令事情更加麻烦的是，杰茜卡的女儿凯特并不希望重新挖出萨默顿男子的尸体。

另外还有一个问题，阿德莱德大学的物理学家德里克·阿博特教授指出，如果要进行DNA测试，我们剩下的时间已经不多了。在《60分钟》节目上，阿博特表示："问题是，如果我们再让萨默顿男子在地下多埋一些时候，比如10年，DNA中的一些非染色体信息就有可能消失。而如果我们想要寻找萨默顿男子的近亲，这些非染色体信息就非常重要。"

事实上，早在这些可能是萨默顿男子亲属的人出现在公众视野中之前，阿博特就曾要求挖出萨默顿男子的尸体进行检测分析。2011年10月，首席检察官约翰·劳（John Rau）驳回了阿博特的第一次掘尸申请，理由是"只有在对公众利益有益的情况下才能掘尸，此处的公众利益不包括公众的好奇心，也不包括广泛的科学兴趣"。注由于出现了可能是萨默顿男子近亲的人，阿博特认为自己申请掘尸的理由更加充分了。于是，2013年11月，阿博特再次向约翰·劳提出申请。阿博特在申请中写道：

> 目前政府致力于确认一些已被埋葬的"一战"和"二战"死者的身份，以给死者的家属最终一个交代。确认这名男子身份的请求也同样符合这一精神。并且在此案中，这样做对公众利益十分有益。注
>
> 具体而言，此举与公众利益的联系是，现有一名可能是该男子后代的人居住在澳大利亚境内。基于历史和解剖证据，我判断此人是萨默顿男子后代的可能性很高。注

遗憾的是，这次阿博特的运气不比上次好。首席检察官劳再次驳回

了他的掘尸申请。曾花费大量时间研究萨默顿男子案的费尔特斯在他的网站上发表了对上述裁决结果的看法：

> 我收到一封来自尊敬的副州长兼首席检察官约翰·劳的信件，信件上所署的日期是2014年3月6日。信中称，基于一系列考虑，他驳回了阿博特教授的掘尸申请，对挖掘萨默顿男子遗体的要求不予批准。我必须说，我和很多人一样支持他的这一决定。德里克·阿博特已经两次申请挖掘萨默顿男子的尸体，两次申请均被驳回。我希望他能够接受首席检察官的这一判决，不要再把他的专业知识用到他职业以外的地方。(注)

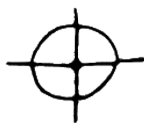
阿博特申请掘尸并不是因为他相信某种阴谋论。事实上，他甚至都不认为萨默顿男子是一名间谍。阿博特表示："大家都喜欢间谍论，但我找不到任何证据来支持萨默顿男子从事间谍活动的说法。你可以去国家档案馆查阅澳大利亚安全情报机构（ASIO）的以往记录——护士杰茜卡以及阿尔弗雷德·博克索尔的名字我们也都认真调查过——根本找不到任何信息。那个时代的所有档案现在都已经公开了。萨默顿男子是间谍的说法实在站不住脚。"(注)

虽然我尊重阿博特的上述意见，但我并不同意他的看法。下面这个例子能够说明我为什么不同意他的看法。詹姆斯·班福德（James Bamford）曾根据信息自由法案（Freedom of Information Act）向美国国家安全局提出申请，要求后者出示所有可能与他有关的档案。美国国家安全局调查后称，没有发现任何与詹姆斯·班福德有关的档案。然而，事后班福德发现自己曾经有过一个代号。于是他再次提出申请，要求美国国家安全局出示与该代号有关的档案，这次他却找到了自己的档案！也许澳大利亚的情报机构不是没有关于萨默顿男子的记录，只是目前还没有人以正确的方式提出过申请。还有一种可能是，情报机构曾有过关于萨默顿男子的记录，但是这些文件被损毁或者丢失了。毕竟，在萨默顿男子案中，记录警方调查情况的许多材料都随着时间的流逝而消失不

见了。

不管我们能否对萨默顿男子进行DNA测试，我们仍有希望最终确认萨默顿男子的身份。如果凯特引用的杰茜卡的话属实（即萨默顿男子的身份是一个只有高层人士才知道的机密），那么随着更多澳大利亚情报被解密，也许在未来某个时候，揭示萨默顿男子身份的文件会被公之于众。如果萨默顿男子真是一名苏联间谍，既然冷战已经结束，曾经的社会主义国家的许多档案也已经逐步解密，我们就可以寄希望于获得更多关于萨默顿男子身份的新线索。我个人的看法是，萨默顿男子的身份最终会公开，但是那本《鲁拜集》中的密码却可能永远无法解开。

保罗·鲁宾案



机场里的尸体

1953年1月20日上午快到10：00时，美国陆军二等兵马德里·金（Madrid King）在去往费城国际机场的时候，在一个深达12英尺的陡沟里发现了一具尸体。

大约在尸体被发现前20分钟，一名证人还看到死者在机场中走动。这名证人是罗伯特·M.安德森（Robert M.Anderson）神父。据安德森神父描述，死者是一名“身材结实的男子”，“年龄在25~30岁之间”，[注]“眼神惊恐”。[注]安德森神父这样描述他遇到这名男子时的情形：

> 当时，他正在航站楼和机场快车办公室之间的坡道上。我对他说：“早上好。”他没有回答，而是继续来回地走动。当时，我注意到他直直地盯着前方，而且他的瞳孔有放大的迹象。注

在另一篇报纸的报道中，安德森神父称这名男子“看起来有些紧张”。注

这名看起来有些紧张、激动的男人当时是否知道自己的生命马上就要走到尽头了呢？

在这个案子里，答案很少，问题却很多。事实上，就连我在上面列出的这些基本事实也并不是完全确定的。根据另一个来源，发现尸体的人不是一名士兵，而是一名出租车司机。对于一些细节也有许多不同的说法。比如，有的来源称发现尸体的沟深度大约是10英尺。注在下文中，我们还会继续看到，本案中的许多简单的事实都出现了多种互相矛盾的说法。

在沟中发现的这名男子的尸体上找不到任何身份证明文件。根据验尸官约瑟夫·奥明斯基（Joseph Ominsky）以及警方情报组的领导詹姆斯·麦克塔格（James McTague）警官的估计，死者的年龄大约在25~30岁之间。关于死者的身高有许多不同的说法，有的报告称死者的身高是5英尺10英寸，也有的报告称死者的身高是6英尺，还有其他一些报告中列出的身高在上述两个数值之间。死者的体重在190~200磅（约86~91千克）之间，他的头发和眼睛都是棕色的。在死者身上没有发现暴力的痕迹。死者所穿的运动外套上有一个标签，上面写着“维特兄弟，第五大道”。注根据这条线索，警方将调查的方向转向了纽约。

死因是氰化物中毒

尸体解剖未能确定死者的死因，但是化学家们却提出了毫无疑义的

结论。

警方犯罪实验室的爱德华·伯克（Edward Burk）医生发现，死者身上有氰化钾中毒的痕迹。根据验尸官约瑟夫·奥明斯基的说法，死者体内的氰化物含量足够“杀死10个人”。[注]在摄入毒药以后，死者几乎是立刻死亡。奥明斯基还说：“这可能不是自杀。致死的毒物可能不是死者自行服下的。尸体的状态显得过分整齐了，甚至死者佩戴的那副镜片很厚的眼镜也还保持在脸上的正确位置上。如果死者在服毒后自己跌倒，那上述情况是不太可能出现的。根据这些情况判断，死者的尸体有可能是被其他人放置在该地点的。”[注]

奥明斯基还说：致死的氰化物“不是常见的类型——氰化物中还混有其他药剂”，但他并没有进一步透露“其他药剂”究竟是什么药剂。[注]

在沟的斜坡上发现了一块白色的手帕，发现手帕的地点距离沟的底部大约有10英尺的距离。这条手帕是不是在死者的尸体被放入沟中的时候掉出来的呢？

除了死者的体格以外，关于死者的外形还有另一处令人印象深刻的细节——那就是奥明斯基提到的那副镜片很厚的眼镜。不同的文献对这副眼镜的描述也有所不同，我找到了以下这些不同的说法：

> “厚厚的塑料框眼镜”[注]
>
> “很厚的牛角框眼镜”[注]
>
> “玳瑁壳的眼镜”[注]

但是不管镜框到底是什么样的，可以确定的是这副眼镜的镜片肯定非常厚。麦克塔格警探说：“死者的眼镜很奇怪，镜片厚得简直像是两片放大镜。”[注]

假如你想干坏事，且不希望目击证人向警方准确描述你的样貌，方

法之一就是在身上制造出某种非常戏剧化的特点，这样目击证人就会只记得这种戏剧化的特点，而完全忘掉你的其他特征。也许死者身上的这副奇怪的眼镜就起到了这样的作用。

而死者服用氰化物的方式也一直是个谜。

有一份报告称："根据奥明斯基的说法，不管是在案发现场还是在这个年轻人的口袋里，都找不到任何小瓶或者其他容器。"[注]然而，第二天又有一份报告称，在尸体旁边大约5英尺的地方发现了一个"5英寸长的试管"。[注]警方怎么可能漏掉这么明显的证物呢？更奇怪的是，在这个试管中并没有检查出任何毒药的痕迹，而且也没有找到这个试管的瓶塞或者瓶盖。

然而，还有一个来源称："警方声称在死者身上找到了一个打碎的小玻璃瓶。"[注]

奥明斯基称，死者服下的毒药可能是以胶囊形式服下的，也可能是以粉末形式服下的。此外，他还说："到目前为止，我们还没有找到任何证据能证明死者服下的毒物是装在胶囊里的。约翰·S.希恩（John S.Shinn）医生将对死者的尸体进行第二次解剖，并试图找到包裹毒物的胶囊的痕迹。"[注]从上述这些信息看，致死的毒药似乎并不是以胶囊的形式被死者服下的。

美国联邦调查局将死者的指纹发送给华盛顿和纽约（因为死者所穿的运动外套上标有纽约的店铺名称）的警方，然而警方并没有找到与死者的指纹相匹配的记录。

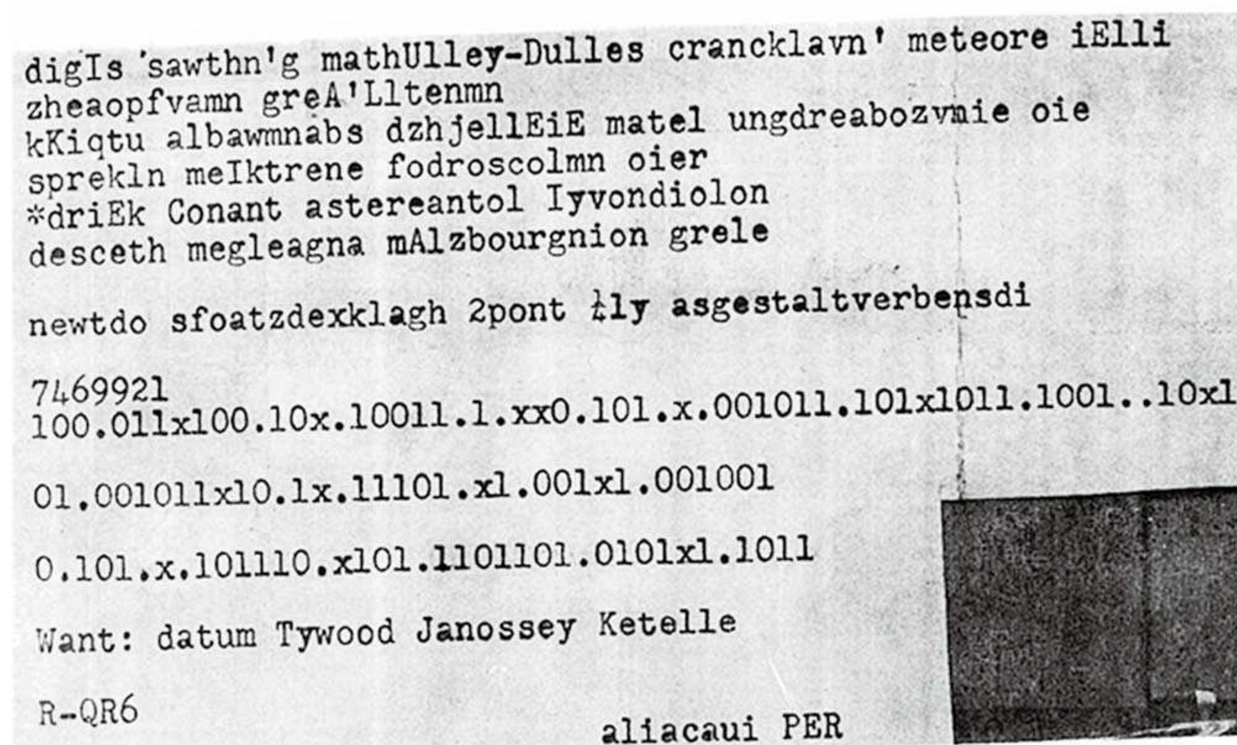
一段隐藏的密码

在死者身体的另一部分，警方还发现了另一条线索。死者的腹部贴有一条6英寸长、2英寸宽的胶带。当警方从死者身上取下这条胶带时，

一张压在胶带下方的卷起的纸片掉到了地上。打开这张纸片以后，警方发现这张7英寸长、3英寸宽的纸片上有一段经过加密的信息。(注)

美国联邦调查局的介入

在这张神秘的纸片上出现了两个名字（这两个名字似乎是用明文写成的），这两个名字让警方决定联系美国联邦调查局。纸片上的这两个名字分别是“杜勒斯”（Dulles）和“科南特”（Conant）。当时，约翰·福斯特·杜勒斯（John Foster Dulles）刚刚被艾森豪威尔总统任命为美国的新任国务卿，而詹姆斯·B.科南特（James B.Conant）博士则是哈佛大学校长，他当时刚被提名出任美国驻联邦德国的高级专员。


digIs 'sawthn'g mathUlley-Dulles crancklavn' meteore iElli
zheaopfvamn greA'Lltenmn
kKiqtu albawmnabs dzhjellEiE matel ungdreabozvmie oie
sprekln meIktrene fodroscolmn oier
*driEk Conant astereantol Iyvondiolon
desceth megleagna mAlzbourgnion grele

newtdo sfoatzdexklagh 2pont ly asgestaltverbensdi

7469921
100.011x100.10x.10011.1.xx0.101.x.001011.101x1011.1001..10xl

01.001011x10.1x.11101.xl.001xl.001001

0.101.x.101110.x101.1101101.0101xl.1011

Want: datum Tywood Janossey Ketelle

R-QR6

aliacaui PER

图6-20 贴在神秘男子腹部的密码

虽然所有关于本案的报纸报道都对“杜勒斯”和“科南特”这两个名字指代的身份毫无疑义，但事实上这两个名字也未必就一定是指以上两位

政治人物。美国国家安全局历史学家戴维·哈奇（David Hatch）指出，“杜勒斯”也可能指其他政治人物，比如约翰·福斯特·杜勒斯的兄弟、即将出任美国中央情报局局长的艾伦·杜勒斯（Allen Dulles），或者美国国务院分管西德事务的干事埃莉诺·杜勒斯（Eleanor Dulles）。注

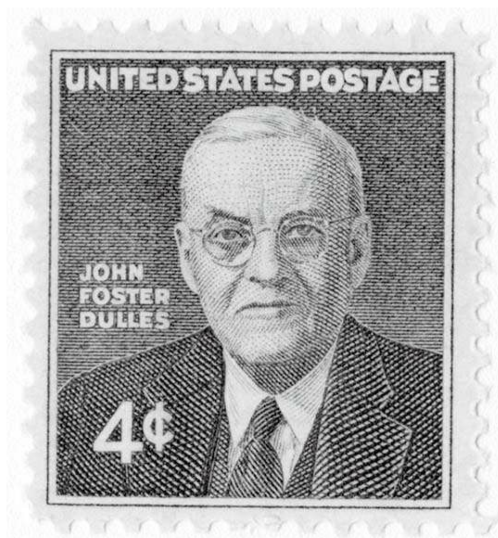


图6-21 1960年的一枚纪念杜勒斯的美国邮票



图6-22 1953年2月18日的詹姆斯·B.科南特

与德国的秘密联系

另一条将此案与德国联系起来的线索出现在死者的仿鳄鱼皮钱包中。㊟死者钱包中装的不是女朋友的照片，而是一架飞机的照片，飞机的尾翼组上漆着纳粹的标志。这张照片的背面写着“France Field, Panama（法国战场，巴拿马）”的字样。死者的钱包中共有2张照片，另一张照片是罗丹的著名雕塑《思想者》。

如果这名神秘男子是自己服用氰化物自杀的话，那么这种自杀方式与大约10年前许多纳粹高层人员采用的自杀方式非常相似。1944年，埃尔温·隆美尔（Erwin Rommel）服用氰化物自杀。1945年，海因里希·希姆莱（Heinrich Himmler）、阿道夫·希特勒（Adolf Hitler）、埃娃·布劳恩（Eva Braun）也都服用了氰化物自杀。当然，希特勒除了服毒以外还对自己开了枪。1946年，赫尔曼·戈林（Hermann Göring）也服用氰化物胶囊自杀。约瑟夫·戈培尔（Joseph Goebbels）给自己6个孩子分别服下了氰化物（这实在是太可怕了！），然后自己也服下氰化物自杀（这一点我们倒是不介意）。

读者可能还记得，此前我们提到有一位名叫安德森神父的证人称，他曾向死者打过招呼，然而他对死者说“早上好”以后，死者却完全没有回答。一种可能的解释是，死者有很强的德国口音，并且不希望别人发现这一点，所以他才选择不回应安德森神父的问候。

死者身上的其他物品

在死者身上，警方还找到了以下这些物品㊟：

1. 一个塑料圆筒，圆筒里有一根信号保险丝

2. 一枚用过的0.38英寸口径子弹的弹壳（在死者的大衣口袋中）

3. 一支钢笔枪

4. 47美分

5. 一条钥匙链，上面有4把钥匙，其中一把可能是别克牌汽车的钥匙㊟

其中第3件证物值得好好研究一下。詹姆斯·麦克塔格警官对这件证物做了如下的描述：

> 死者身上还有一支钢笔枪或铅笔枪。我们正在调查这支枪究竟是什么类型的枪。它看起来有点儿像气枪，又有点儿像其他种类的枪。它的两头较钝，有一个用于发射子弹的撞针。㊟

如果说一名警官都需要经过进一步调查才能搞清楚这是何种枪支的话，这种型号一定非常少见了！

此外，在死者身上还发现了另一件没那么可疑的东西，那就是一本当年2月号的《星系科幻小说》（*Galaxy Science Fiction*）杂志。据报告称："警方人员称，这本杂志中的一篇小说——贝尔博士所写的《神秘数字》的内容与密码有关。"㊟数学家E.T.贝尔（E.T.Bell）的确用笔名约翰·泰恩（John Taine）来写科幻小说，但是1953年2月号的《星系科幻小说》杂志中并没有一篇贝尔博士所写的名为《神秘数字》的小说，并且这本杂志中也没有任何内容与暗号或者密码有关。此外，还有报道称，警官表示杜勒

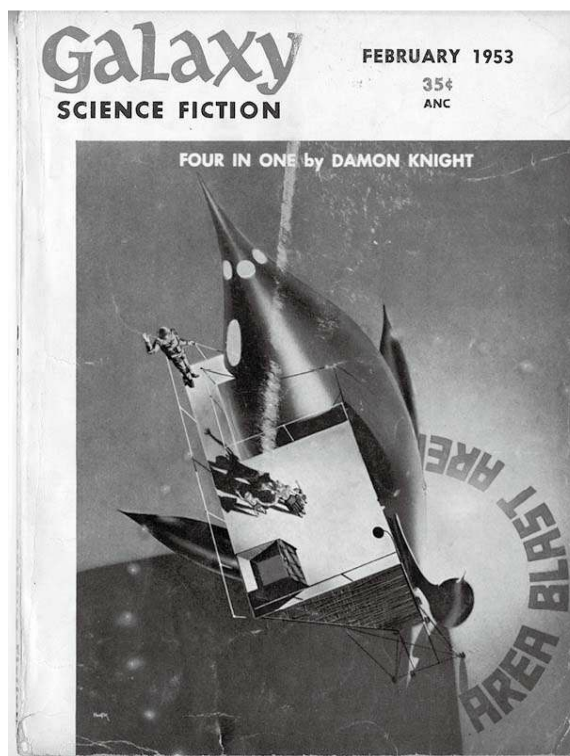


图6-23 一本内容与报告不符的科幻杂志

斯和科南特的名字出现在这本杂志中的其他小说中，但这种说法也是不正确的。注

死者身份的确认

据估计，死者的年龄在25~30岁之间，因此在第二次世界大战结束时，死者的年龄应该在17~22岁之间。所以，有人猜测这名体格强壮的神秘男子可能是一名经过“二战”洗礼的士兵。在战争结束以后，也许他选择继续为自己的祖国德国服务，在美国从事间谍活动。然而，警方最终确认了死者的身份。事实上死者是一名来自纽约布鲁克林区的犹太青年。为什么一个犹太人的钱包中会放着纳粹飞机的照片呢？这个问题一直都没有得到解释。

警方确认死者身份的过程如下：1月20日，居住在纽约布鲁克林区的贝西·鲁宾（Bessie Rubin）在报纸上读到了费城机场发现尸体的新闻，而她的儿子于前一天——1月19日，星期一——失踪。贝西最后一次见到儿子的时间是1月19日早上9：30。

于是，贝西致电费城警方，表示在费城机场发现的男子的特征与自己的儿子类似。贝西提到，她的儿子佩戴着镜片很厚的眼镜，这一点与死者的外貌描述完全一致；贝西还提到，她儿子的身高是5英尺11英寸，体重是175磅（约79千克，比死者的估计体重略轻一些），年龄是18岁。贝西的儿子的实际年龄似乎比警方估计的死者年龄要小很多。关于这一点，贝西表示，自己的儿子看起来比实际年龄要成熟一些。此外，死者身上穿着的衣物也与贝西描述的穿着基本类似。

据报道称，警方在费城的停尸房中拍摄了死者尸体的照片，并且将这些照片“通过本地联邦调查局办公室的有线照片传真机传给了纽约总部”。然后，纽约方面的人员向贝西展示了这些照片，并希望通过这种方式确定死者的身份。注

然而，官方文件中的记录却是这样的：接下来贝西·鲁宾和她的丈夫塞缪尔（Samuel）以及她的兄弟马克斯·格斯特曼（Max Gerstman）一起来到了费城。1月21日下午3点，塞缪尔在费城的停尸房中确认了儿子的尸体。在看到尸体之前，贝西就晕倒了。

至此，警方已经确认死者就是18岁的保罗·伊曼纽尔·鲁宾（Paul Emanuel Rubin）[注]。死者身份的确认解决了一个谜团，却没有办法解决另一个谜团——这个孩子究竟在费城机场干什么？

据保罗·鲁宾的父母称，保罗从童年时期开始就喜欢给朋友们发送加密信息。因此，他身上发现的这段密码可能不是别人发给他的，而是他自己写的。此外，保罗的母亲还回忆起，1月19日早晨保罗离开家之前，她曾看到儿子用刀割下了几条胶带。然而，保罗的父母都无法破译儿子留下的最后一段密码。

除了保罗的父母以外，警方还询问了保罗的一位朋友，文件中没有详细记录这位朋友的身份。警方希望保罗的这位朋友能够解释在保罗身上发现的密码。

> 保罗的这位朋友告诉警方，鲁宾和其他年轻人一直在从事与密码有关的活动，并且他还声称，如果能找到正确的密码本，自己也许可能破译在保罗尸体上发现的密码。他说，这项工作可能要花费他一个星期的时间。保罗的这位朋友还补充说："这些东西是很复杂的，任何读科幻小说的人都能明白我的意思。"……这位朋友无法解释保罗为什么会死亡，并且他还表示，他怀疑即使破解纸条上的密码，也没有办法找到保罗死亡的真相。[注]

文件中并没有记载保罗的这位未公开身份的朋友究竟花了多少精力来破译保罗身上的这段密码。但是美国联邦调查局费城办公室却非常严肃地对待了保罗身上的这段密码。费城办公室将这段密码发送给了华盛顿的密码分析专家。

保罗星期一早上离开家时，他的父母以为儿子要去纽约大学。保罗是纽约大学化学系的一名大二学生。由于保罗的专业是化学，我们几乎可以肯定他要么自己可以接触到氰化物，要么认识某个能够接触到氰化物的人。因此，似乎不能排除保罗服用氰化物自杀的可能性。然而，贝西说，在保罗星期一早上离开家的时候，他看起来身体健康，精神状态也很好，完全没有迹象显示他在为什么事情担心。并且，贝西还说，保罗离开家时，他身上还有15美元的现金。那么，为什么保罗的尸体被发现时身上只有47美分呢？㊟余下的14.53美元究竟去了哪里？此外，在保罗身上发现的其他奇怪物件又应该怎么解释呢？

塞缪尔和贝西对保罗身上的其他物件是这样解释的：

> 保罗的父母说，保罗经常练习一种魔术表演。在保罗口袋里发现的长条圆筒形信管（上面连着电线）可能是他经常练习的魔术表演中使用的一个道具。㊟
>
> 保罗的父母还认出，钥匙圈上的4把钥匙中有一把是他家的一辆旧汽车钥匙，这辆旧汽车目前已经不在家了。此外。在同一个口袋中还发现了一个空弹壳。保罗的父母说，这个弹壳可能是保罗从一位喜欢射击的朋友那里拿来的，保罗可能是打算用自己混合的火药来帮朋友重新装好这个空弹壳。㊟

贝西表示，除了对魔术感兴趣以外，保罗还喜欢“沉重的文学作品”以及“有关飞机的知识”。㊟后一点也许可以解释保罗的钱包中为什么会有一张带有纳粹标志的飞机照片。然而，世界上的飞机有那么多种，为什么保罗偏偏选择了这架飞机呢？还有，照片背后的字样又是什么意思呢？

除了上面这些细节，贝西还提到，她的儿子保罗是一名非常聪明的学生，他很喜欢下棋，对国际事务也很感兴趣。保罗与纽约市的许多外国学生关系密切，也经常谈到自己与纽约大学里的外国学生之间的友

谊。保罗的父母说，保罗从来没有把这些外国学生带回家里过。但是，贝西提到，保罗“常常将一些装着奇怪液体的罐子带回家里”。贝西称自己从来不知道这些罐子里究竟装着什么。注

显然，保罗父母的上述这些说明都不能解释保罗身上为什么会有一支钢笔枪。虽然这个问题以及许多其他重要问题的答案都没有找到，但是保罗·鲁宾的尸体在确认身份以后被送回了纽约市的布鲁克林区，并被他的家人按照犹太传统习俗埋葬了。

纽约大学提供的其他线索

1月23日，《费城询问报》（*Philadelphia Inquirer*）的报道称，费城警方凶案组的迈克尔·施瓦茨（Michael Schwartz）警官表示，已经要求纽约警方询问纽约大学的学生和教职人员，希望搞清楚星期一早晨保罗究竟有没有去纽约大学上课。另一份报纸也跟踪报道了这方面的进展，称：“警方称，他们发现，保罗的一些学生朋友在保罗失踪前曾看到他用剪刀剪胶带。”注我们不难看出，这条信息有些奇怪。因为保罗的母亲曾说，在保罗离开家之前，她就曾看到儿子用刀割胶带。难道是用胶带粘上的密码掉了下来，需要重新剪胶带贴上吗？

此外，警方在纽约大学的调查讯问还找到了其他一些有价值的信息。1月27日，奥明斯基提出保罗可能是因为受别人欺负才选择自杀。奥明斯基表示，他和弗兰克·A.利文索尔（Frank A.Levinthal）警官与纽约大学的教职员工以及死者的亲戚和朋友进行了许多“有趣的对话”。奥明斯基认为，保罗可能因为想要加入一个兄弟会，却未被接纳入会而感到抑郁。注

在案发几十年以后，我自行对此案展开了调查。我联系了纽约大学的档案馆，询问他们是否有任何与此案相关的信息。档案馆的一位研究生助理克莱尔·阿什利·沃尔福德（Claire Ashley Wolford）回复称：“我

查阅了一些报纸，在校报中找不到任何与这起案件有关的信息。”接着，沃尔福德又提到，她发现《纽约时报》[注]上的一篇文章称，保罗·鲁宾是华盛顿广场艺术与科学学院的学生，沃尔福德向我解释说，当时华盛顿广场艺术与科学学院的校区和纽约大学的高地校区分处两个不同的地点。这个结果与我之前的预想完全不同。[注]我本以为，虽然案件发生于纽约大学的另一个校区，但是校报多少应该提到这起案件才对。毕竟，连《生命》（*Life*）杂志都报道了这起案件呢！[注]

除了询问纽约大学的师生以及死者的亲戚朋友以外，奥明斯基还从其他方面展开了对本案的调查。以下是他说的一段话：

> 因为我坚信死者并非死于自杀，所以我联系了联邦调查局，请他们调查死者在纽约和费城的人际关系，以确认死者是否担任某种不正常活动的信使。我相信联邦调查局正在进行这方面的调查，在找到上述问题的答案之前，我无法定下此案死因讨论会的具体时间。[注]

此时，另一条线索解释了保罗是如何从纽约前往费城的，但是这条线索的内容是否准确还有待查证。

一位卡车司机致电爱德华·施里弗（Edward Schriver）警探和弗兰克·凯利（Frank Kelly）警探称，星期一早晨，他在东兰斯当的巴尔的摩收费公路和教堂巷的交界处接到了一名特征与死者吻合的年轻人。那位年轻人说要去华盛顿看总统就职典礼。这名卡车司机称，那位年轻人是在切斯特下的车。[注]

然而，这名卡车司机的证言给我们带来了更多难以回答的问题。如果保罗是想去华盛顿看总统就职典礼，他为什么不事先告诉朋友和家人呢？我不清楚是否有任何一位保罗的朋友或家人在证词中提到保罗要去看总统就职典礼的事情，至少在我能找到的所有新闻报道中都没有出现这条信息。

最终，保罗案的死因讨论会于1953年2月23日举行。但是在这次讨论会上，本案的所有重要问题都没有得到回答。主持此次讨论会的奥明斯基称，警方没有找到任何动机，奥明斯基还说保罗·鲁宾死于“某种目前尚不明确的原因”。没有任何证据能够解释保罗究竟如何到达费城，也没有任何证据能解释他如何服下氰化物。(注)

除了上述几个疑问以外，本案中还存在一些其他问题。这些问题应该都很容易回答，然而我在任何文献中都找不到这些问题的答案。比如，保罗拥有一台打字机，警方调查人员表示，他们会将密码中的字符与该打字机打出的字符进行对比，以确定保罗究竟是密码的制造者还是密码的接收者。鉴于保罗有写密码的习惯，似乎他是密码制造者的可能性较高，如果能找到这个问题的明确答案，将会对本案的侦破工作提供一些帮助。

一篇关于此案的死因讨论会的报纸文章甚至把保罗的死亡事件变得更加扑朔迷离了，因为它提出了一些与此前认定的细节严重不符的事实。这篇报道称：“这位家住布鲁克林区弗农街122号的青年于1月20日被发现死在机场的一条沟中，发现尸体的人是哈里·凯斯勒（Harry Kessler）——一名住在北六街973号的出租车司机。(注)

此前的所有报道和文件都称保罗·鲁宾的尸体是由一名陆军二等兵在去机场的路上发现的。假如这名二等兵是乘坐出租车到达机场的话，上述说法可能还相对好解释一些，然而在所有此前的报道中，都说这名二等兵是步行走向机场时发现尸体的！

在同一篇文章中，还提到凶案组的一名警官埃德温·S.施里弗（Edwin S.Schriver）在死因讨论会上的发言。据这篇报道称，施里弗警官说保罗多门课的成绩不合格，并且有被学校开除的危险。因此施里弗警官认为保罗是自杀。但是保罗的父亲塞缪尔却说保罗16岁就上大学了，虽然“几乎从来不做作业”，却一直成绩优秀。塞缪尔还说，儿子死亡前一天离开家的时候精神状况良好。(注)

图灵之死

在第二次世界大战期间，艾伦·图灵（Alan Turing）是英格兰最顶尖的密码专家。在破译纳粹德国的恩尼格玛密码的过程中，图灵发挥了极其重要的作用。因为恩尼格玛密码的破译，很多德军情报被截获，这些情报对此后的战局发展起到了极为重要的作用。据估计，由于恩尼格玛密码被破获，“二战”的持续时间至少缩短了一年，恩尼格玛密码的破译甚至可能起到了改变战争输赢的作用。在20世纪50年代，所有这些信息都仍然高度保密。因此，虽然图灵因为他在数学研究方面的成果而颇受尊敬，但普通民众却完全不知道他还是本国的战争英雄。1952年，图灵因为同性恋身份被警方逮捕，他面临两个选择，一是进监狱服刑，二是接受激素治疗来“矫正”他的同性恋倾向。图灵选择了接受激素治疗。根据官方的说法，在接受激素治疗以后，图灵陷入了抑郁，最终他吃下一个含有氰化物的苹果自杀身亡。关于图灵的死亡，一些研究者提出了各种阴谋论。

虽然我并不相信这些关于图灵死亡事件的阴谋论，但是我也听说过这些理论。因此，当我第一次听说保罗死于氰化物的奇怪事件时，我立刻对案件的日期做了一个快速的确认。保罗死于1953年1月20日，而图灵死于1954年6月7日。因此，两人的死亡日期相隔大约17个半月。我的个人意见是，由于这两起死亡事件的时间间隔太长，两者之间恐怕并没有显著的关联。

一篇关于保罗死亡事件的新闻报道称：“每年纽约市约有40~50起氰化物致死事件。其中大部分都是自杀事件。”[注]以上还只是纽约市的数据，在全世界范围内，这个数字肯定还要更加巨大。由于每年会发生这么多起氰化物致死事件，这些死亡事件中肯定能找到一些类似的元素，但是这并不表示这些死亡事件之间真的有关联。这篇报道中还提到：“许多著名科学家都选择使用氰化物自杀，这主要是因为氰化物致死的速度非常快。”[注]

这么多年过去以后，仍然有人试图证实图灵死于某种阴谋。比如，彼得·塔切尔（Peter Tatchell）曾写信给戴维·卡梅伦（David Cameron）首相，要求重新调查图灵的死因。显然，塔切尔希望能找到有力的证据来支持自己的上述申请，但他还是诚实地说出了以下这番话：“虽然没有任何证据能证明图灵是被国家特工谋杀的，但是官方从来没有调查过这种可能性，这方面调查的缺失已经是一个非常严重的过失。”注

更多线索

美国密码协会的前主席亨利·兰根（Henry Langen）曾表示，鲁宾密码是他生平遇到的最具挑战性的密码——至少我认为他指的就是鲁宾密码。注意，兰根的以下说法和我们之前描述的案情既有一些极为重要的区别，又具有很高的相似性，因此我认为兰根所指的案件不太可能是其他案件。

> 在过去的22年中，密码是我非常着迷的一项兴趣爱好。我的最高纪录是花6个月的时间解开一段密码。但还有一段密码我从来没有解开过——这段密码不仅我解不开，美国联邦调查局和所有其他专家也都没有解开。这段密码是几年前出现的，当时，费城附近的特拉华河里打捞出了一具年轻男子的尸体。尸体的背部有一个弹孔，弹孔位于两块肩胛骨之间。因此，可以判断该男子不是死于自杀。而男子裸露的腹部用胶带贴着一段加密的信息！注
>
> 当地的密码专家没有能够破译这段密码，于是这段密码被转给了联邦调查局以及全国各地水平较高的密码爱好者们。我花了两年的时间也没有能够破解这段密码。两年以后，我放弃了。但据我所知，还有其他人在继续研究这段密码。如果这段密码最终能被破译的话，也许它能够帮助我们侦破一桩谋杀案。注

有些读者可能会觉得，既然这么多人投入了这么大精力也没能解出鲁宾密码，那么一定是这段密码太难了，其他人就更不可能解出这段密码了。但是，我认为，20世纪50年代以后就再也没有人尝试破译这段密码了，而20世纪50年代的密码专家手中的主要工具只有图纸和2号铅笔。保罗·鲁宾案早已成了一桩被遗忘的案件。我认为，如果哪位读者尝试用今天的计算机技术来破译这段密码的话，成功的希望还是很大的。

由于在关于本案的各种媒体报道中互相矛盾的说法太多，我们急需找出一个新的调查方向。有趣的是，一份报纸为我们提供了一条这方面的线索。(注)

我们发现，有一张拍摄了图6–20所示纸条的照片上方有这样一行字：“密码案件文件　＃540266–15。”（图6–24）这行字可能为研究者提供了一条极有价值的线索，因为这是一个美国联邦调查局的文件档案号码。本章之前提到的萨默顿男子案受到了公众的长期关注，而保罗·鲁宾案却很快就被公众遗忘了。也许关于鲁宾案的警方案卷以及联邦调查局文件早已丢失。如果上述文件仍然存在的话，它们恐怕也已经在某个档案室里尘封几十年了。有了这个文件号码和几篇20世纪50年代的报纸文章，我根据信息自由法案向费城警察局、联邦调查局，以及国家安全局提出了调取鲁宾案档案的申请。费城警察局回复说，由于此案的案卷年代过于久远，他们已经不再保存这件案子的卷宗了。而美国国家安全局则表示没有找到任何与本案有关的文件。然而，联邦调查局的回复却很有价值，他们建议我去查阅国家档案记录管理局（National Archives and Records Administration，简称NARA）的相关材料。在国家档案记录管理局中，普通民众就可以查阅到大量资料，但是关于保罗·鲁宾案的文件目前还没有通过解密审查，因此没有公开。于是，我很自然地向国家档案记录管理局申请查阅上述文件。不久之后，我收到了国家档案记录管理局的回信，这封回信包括以下这样一段文字：

你申请调阅美国联邦调查局总部的案件文件，文件编码为65－HQ－61458。根据联邦调查局的鉴定，上述编号的文件可能与你要求调阅的保罗·E.鲁宾的案卷有关。我们在第1123号文件盒中记录条目号为569603（US－07D 2）的位置找到了这份文件。该文件属于记录组65：美国联邦调查局记录；分类65（间谍），总部案件文件，1936—1978。上述文件的主题是保罗·伊曼纽尔·鲁宾，文件包括两个部分（第1部分，和附属部分A），上述文件估计共有160页。该文件被汇编为以下文件分类的一部分：1953年1月至1953年3月期间进行的内部安全调查。

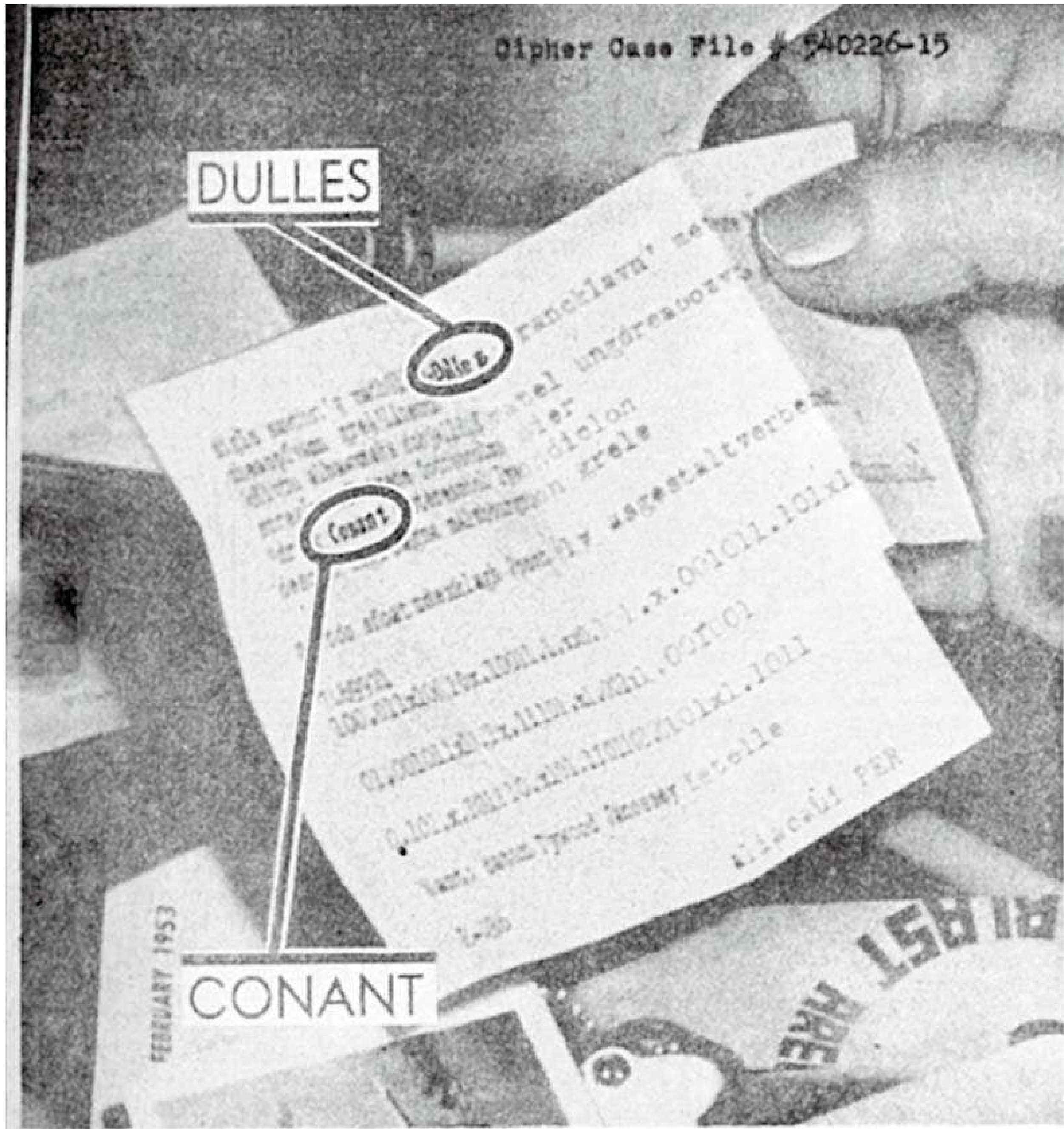


图6-24 报纸上的一张照片提供了一条新线索

单单是对文件内容的上述描述已经给我们提供了大量信息！如果保罗·鲁宾案只是一次单纯的自杀事件，美国联邦调查局会花3个月的时间调查本案，并且写出160页的相关案卷吗？我认为这种可能性不大。此外，从以上的这封回信中我们还可以看出，美国联邦调查局将保罗·鲁

宾案归为间谍案件。

国家档案记录管理局在这封回信之后还附上了上述文件的16页内容。不幸的是，这16页全部都是关于鲁宾案的新闻报道。由于保罗·鲁宾案的卷宗在公开前需要经过审查，所以目前还不能供公众调阅，但显然关于此案的新闻报道并不是什么保密内容，因为它们从一开始就是公开的信息。

虽然我们非常想要知道美国联邦调查局究竟在破译鲁宾密码的工作上取得了哪些进展，但现在我们只能继续耐心等待文件的其余部分被公开。然而，与此同时，我们也可以尝试自己来破解鲁宾密码。

鲁宾密码的数字部分是一种我从来没有见过的密码类型。我期待读者能向我提供一些破译的想法！接下来，我想向读者展示如何通过几种简单的统计检验来对鲁宾密码的字母部分提出假说。

如果我们只统计密码中的字母，而忽略空格的话，鲁宾密码的上半部分（还没有大量数字出现的那部分）的字母频率与正常英文的字母概率非常接近。从图6–25中的柱状图中可以清楚地看到这一点。

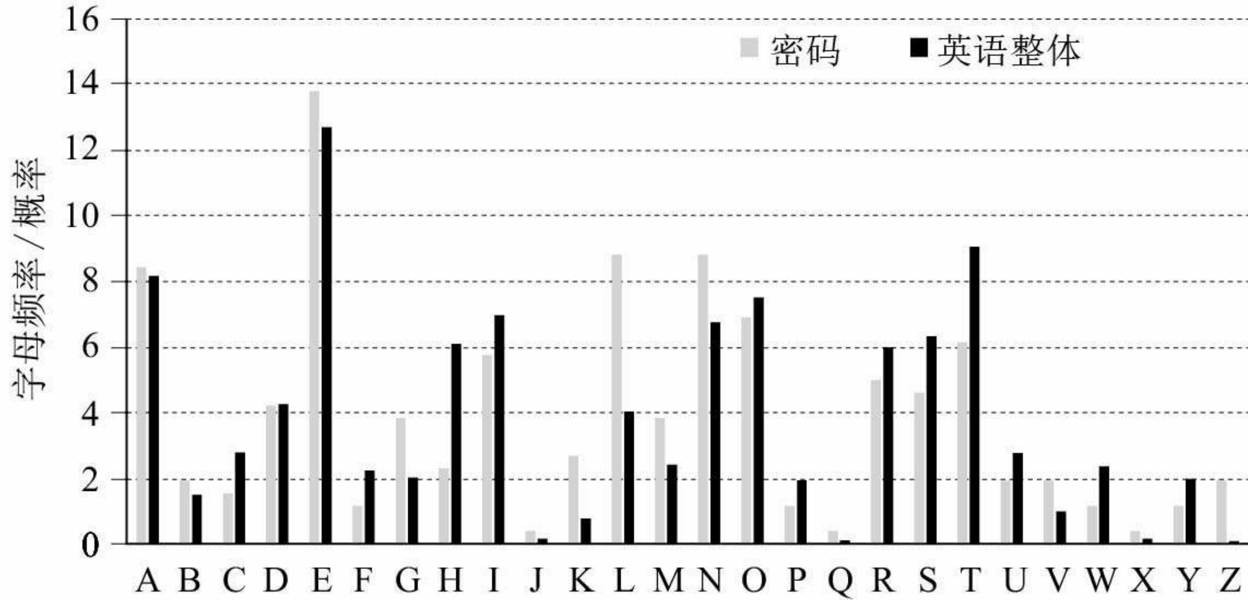


图6-25 密码字母频率（浅色）和英语整体字母概率（深色）的对比

当然，密码的字母概率并不能完全与正常英文的字母概率相匹配。

比如，和正常英文相比，密码中字母H和字母T的数量太少，而字母K、字母L和字母Z的数量则太多。如果这段密码是以“电报体”写成的话，就能够解释密码中字母H和字母T数量偏少的现象。发电报的时候，邮局通常是按电报的词数计价的，因此在写电报内容的时候，人们通常会省去正常英文中经常出现的冠词“THE”。这样，电报的意思仍然很清楚，但发电报的人却可以少付一些电报费。如果多次省略冠词“THE”，字母T、字母H和字母E出现的概率就会下降。虽然在这段密码中，事实上字母E出现的概率比正常英文中字母E出现的概率还要稍高一些，但是我们的上述假说看起来仍然是有一定道理的。既然在这段密码中，大部分字母的概率与正常英文一致，而两个特例字母（即字母T和字母H）的概率又能被一种简单的假说解释，那么我们就可以得到一个显而易见的结论，那就是：这段密码可能是一种换位重排密码。但是，我们还需要考虑另外一项统计结果。

注意，在这段密码中是有空格的。假设我们暂时忽略所有标点符号和数字，那么这段密码的初始部分共包含261个字母，这261个字母被分成了31个“单词”。也就是说，平均每个单词包含8.4个字母。在本书的第1章中我们曾经提到，正常英语单词的平均长度是5.1个字母。[注]因此，显然这段密码中的单词太长了。如果这段密码只是调换了字母和空格的顺序的话，单词的平均长度并不应该发生变化。

为了解释这种统计现象，我们可以提出另一种假说，那就是：加密者在这段密码中加入了一些无效字符。在之前的章节中我曾经解释过，所谓无效字符就是在密码中加入一些和信息本身无关的字符。当密码接收者破译密码时，要完全忽略这些无意义的字符。虽然这段密码中的任何字符都可能是无效字符，但是加密者似乎过多地使用了K、L、Z这3个字母（因此密码中这3个字母出现的频率才会高于正常英文中的概率）。如果你看一看今天的电脑键盘（其字母排列顺序和20世纪50年代的打字机一样），就会发现第2行的最后两个字母是K和L，接着第3行的第1个字母是Z。虽然这可能只是一种巧合，但是注意在这段密码中J、K、L、Z、X这5个字母出现的概率都高于在正常英文中的概率，而

这5个字母在键盘上是连在一起的。也许这并不是一种巧合！

当然，我无法向读者提供鲁宾密码的完整解法。如果我能够破译鲁宾密码的话，它也就不能算是未解之谜，也就不会被我写进本书了。但是，上面的这些统计分析使我怀疑，鲁宾密码的加密者采用了以下这种加密方式。我个人的猜测是：加密者没有改变原始明文信息中的任何字母，而是在这些字母中插入了许多无效字母。在插入无效字母时，加密者故意让这些无效字母的出现概率与正常英文中的字母概率保持大体的一致。也就是说，常用字母作为无效字母出现的次数也比不常用字母多。上述加密方式不仅会使密码中每个单词的平均字母数变大，还能误导破译者将这段密码错误地判断为换位重排密码。但由于某些原因，加密者过度使用了J、K、L、Z、X这5个字母。

如果加密者使用的确实是上述这种加密方法，我们可以通过删除无效字母来得到密码的明文。然而，通过这种破译方法所得到的解法有很多。比如，密码的第一行明文可能是：I SAW DULLES RAN TO ELI（我看到杜勒斯跑向了埃利）。我认为这句话不是鲁宾密码第一行的正确解法，但是我很想看看如何用这种方式来解出其他可能的内容。

鲁宾密码的密文中出现了“mAlzbourgnion”一词。这个词一下就引起了我的注意。我认为这个词很像“Mauborgne”（莫博涅）这个名字，而莫博涅是密码学中的工具“一次性密码本”的发明者之一。也许在这段密码中，加密者还使用了一层额外的加密手段，那就是：在插入无效字母之前先改变某些单词的拼法。

此外，我还怀疑密文中的“Conant”并不代表科南特这个名字，这个词对应的明文可能是“Cant”（不能），甚至可能是“Cat”（猫）、“Cot”（吊床）、“Can”（能）之类的单词。

此外，有些读者可能还会注意到，这段密码中似乎掺入了一些德语。我找到的疑似德语的单词包括“sprekln”和“asgestaltverbensdi”。“sprekln”像是德语单词“sprechen”（意为“说”）。而“asgestal- tverbensdi”似乎混合了两个

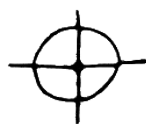
德语单词："gestalt"（意为"形状"）和"verben"（意为"动词"）。假如加密者真的在这段密码中自由地插入了一些无效字母的话，那么他可能是一位玩心比较重的加密者，在加密的过程中，他将无效字母和信息中原本的字母混合在一起，使得密文的单词看起来像是英语和德语中实际存在的某些单词。

我个人的看法是：萨默顿男子密码中的字母数量过少，因此萨默顿男子密码可能永远无法被解开。而鲁宾密码中的字母数量较多（加密者可能插入了100个无效字母），因此我相信鲁宾密码总有一天会被解开。你是否会是迎接这一挑战的那个人呢？

也许，在解开了这段密码以后，我们就能最终搞清楚在1953年1月20日那天，保罗·鲁宾究竟为什么没有去学校上课。

在本书审稿期间，我之前根据信息自由法案要求调阅联邦调查局文件的申请终于收到了回复。我看到的文件只做了几处轻微的删改，以保护一名与本案调查有关的中央情报局雇员的身份。在这份文件中出现了一些新的情节，比如保罗曾经使用过假名。但虽然联邦调查局尽了力，他们最终并未能破译出鲁宾尸体上的密码。在此，我决定不对这份文件的内容进行总结，而是把这份文件完整地放在普林斯顿大学出版社为本书创办的网站上。该网站的网址为：http://press.princeton.edu/titles/10949.html。有兴趣的读者可以下载这份文件，并自行对文件中的细节进行进一步的研究。

麦考密克案



贫民区中的故事

本章的第3名受害者名叫里基·麦考密克（Ricky McCormick）。他生于1958年6月14日，在一个贫困的家庭长大，未来改善自己生活水平的希望也很渺茫。里基的母亲弗朗姬·斯帕克斯（Frankie Sparks）称他是个“弱智”。而与里基关系非常亲近的一位表亲则怀疑他患有双向情感障碍或者精神分裂症。里基从儿童时代开始就有哮喘和胸痛的症状。虽然里基几乎不会读书和写字，但他还是升入了圣路易斯的马丁·路德·金高中，但并没能从该高中毕业。作为一名辍学少年，里基自然只能找一些粗重的体力活干。他干过各种体力活。同时，因为他患有慢性心脏疾病，还从福利机构领取残疾补助金。从大约10岁开始，他就养成了每天至少抽一包烟的习惯，此外，他每天还会喝大约20杯含咖啡因的饮料，显然这些习惯对他的健康不会有什么好处。

一开始，里基还尝试避免与犯罪活动扯上关系。在他居住的街区，经常有暴徒在他家附近打架或者交易毒品。在青少年时期，他常常会乘公共汽车或者沿途搭车以躲开这些暴徒。甚至在成年以后，他有时仍然会这么做。



图6-26 里基•麦考密克

虽然里基·麦考密克并没有暴力倾向，但是由于他智商较低，面临的选择又十分有限，所以他在人生中还是难免犯下一些严重的错误。1992年11月，圣路易斯警方逮捕了他，被捕时他34岁，与一名未成年女孩育有两名子女。从这名女孩11岁起，麦考密克就开始和她发生性

关系。面对警方的指控，麦考密克选择认罪，并被判处3年徒刑。[注] 13个月后，他被提前释放。[注]

重案组的汤姆·奥康纳（Tom O’Connor）警官说，实际上麦考密克至少有4名子女，但他从未透露过另外两名子女的母亲是谁。麦考密克从未结过婚。

麦考密克在圣路易斯有一处住址，在圣路易斯附近的贝尔维尔及费尔维尤高地还有其他几处住址，在伊利诺伊也有另外几处住址。很多像他这样在许多住址之间辗转的人实际上是没有固定住所的流浪汉，他们只是哪里能住就在哪里住下而已。但是，根据圣查尔斯县的治安官助理警官凯文·威尔逊（Kevin Wilson）的说法，麦考密克虽然无业并一直在领取政府的残疾人补助，但他并不是无家可归的流浪汉。

生命最后的日子

20世纪90年代末，麦考密克制造了更多麻烦。他会不时前往佛罗里达州。他的女友桑德拉·琼斯（Sandra Jones）说，麦考密克去佛罗里达州是为了买大麻。麦考密克会把大麻带回他和琼斯住的政府保障房，然后用封口塑料袋来分装大麻。他告诉琼斯，这些大麻是留给巴哈·哈姆达拉（Baha Hamdallah）的。各种证据显示，麦考密克本人并不吸毒，甚至连酒都不喝，但是被人们称作“鲍勃”的巴哈却是一个比毒品和酒精更危险的人。

克里斯托弗·特里托（Christopher Tritto）写了一篇关于麦考密克案的最详细的文章。虽然威尔逊警官称麦考密克没有工作，但是特里托却说麦考密克在圣路易斯市中心舒托路1401号的美国石油公司加油站工作，他的雇主就是巴哈·哈姆达拉。也许，麦考密克最先从事的是加油站的正经工作，后来他才发现在巴哈手下还有更好的生财之道。

不管怎么样，我们明确知道巴哈是有暴力犯罪历史的。1997年，一

名警官看见巴哈在自己的车里向另一个男人开枪。巴哈因此被捕，但是没有被提起诉讼。1998年3月，据称巴哈在与他的兄弟巴赫贾特（Bahjat）发生争执以后对他的兄弟开了枪。巴赫贾特声称不认识对自己开枪的人，但是他对凶手的描述与其他证人的证词矛盾（其中包括一名认识巴哈的证人）。［麦考密克死后两个月，据称巴哈被哈姆达拉家的另一个兄弟朱马（Juma）枪击，这次轮到巴哈包庇凶手了。］同样是在1998年3月，巴哈因为用榔头击打他人而被捕。此案为巴哈的暴力犯罪史添上了不一样的一笔，这次巴哈袭击的人不是他的亲属，冲突双方也没有开火。然而，在巴哈出庭受审两周前，此案的受害者被枪杀，巴哈也因此未被定罪。警方的线人称，这起谋杀是“巴哈指示的”。哈姆达拉家的另一个兄弟贾梅尔（Jameil）是警方登记在案的性犯罪者。㊟

虽然美国有些州已经把大麻合法化了，但是在20世纪90年代，大麻在美国的所有50个州都是不合法的。因此，如果麦考密克在贩毒的过程中出了什么差错而被警方抓住的话，不仅他自己会面临重刑，他的老板巴哈肯定也会给他好看。此外，麦考密克还面临着与他竞争的其他毒贩的威胁。

麦考密克最后一次动身去佛罗里达州奥兰多市是在1999年6月15日。当时，他在圣路易斯市中心的灰狗长途汽车站买了一张去佛罗里达的单程票。

在奥兰多停留期间，麦考密克至少给他工作的加油站打过一次电话。琼斯没有透露她认为这通电话里说了什么，但暗示她认为麦考密克可能在最后一次佛罗里达之旅中犯了什么错误。琼斯说，当麦考密克回到圣路易斯的时候，他看起来有些害怕。

从麦考密克回到圣路易斯以后的行为来看，他似乎想要藏起来，不让别人发现他的行踪。虽然警方未能完全搞清楚麦考密克在圣路易斯区域内四处躲藏的具体细节，但是从警方掌握的信息中，我们已经可以充分感受到麦考密克的恐惧了。

6月22日下午，麦考密克走进了巴恩斯犹太医院的急诊室，声称自己胸部疼痛并且呼吸困难。医院收治了他。麦考密克住了两天院之后于6月24日出院。出院后，他的下一站是格洛丽亚阿姨家，他搭乘公共汽车来到格洛丽亚阿姨家，但是只在那里待了大约1个小时。

6月25日下午5点，麦考密克走进了另一家医院（森林公园医院）的急诊室，再次声称自己呼吸困难。如果他此举的目的是希望在医院过夜的话，那么他失算了。1个小时以后，医院就让他出了院。麦考密克的阿姨格洛丽亚听说他在医院的候诊室中过了一夜。一般来说，病人都会迫不及待地盼着出院。如果麦考密克不是不敢回家的话，他为什么要在医院的候诊室里待一整夜呢？

第二天早上11：30左右，琼斯和麦考密克通了电话。麦考密克说，他正准备前往工作的加油站弄一点儿吃的。警方并不清楚当天麦考密克究竟有没有去加油站，但是根据一位被警方讯问的美国石油公司加油站员工的证词，麦考密克在6月27日确实去过加油站。(注)这是警方知道的麦考密克死前到过的最后一个地点。警方的验尸人员确定麦考密克于当天的某个时间死亡。如果麦考密克当时正在躲避巴哈的话（从他选择在医院候诊室过夜而不回家来看，我们似乎可以做出这种推测），那么为什么他最终还是回到了加油站呢？也许，麦考密克得到了巴哈的虚假承诺，以为巴哈已经原谅了他在奥兰多犯下的错误。

虽然琼斯似乎知道这方面的情况，但她看起来并不想向警方透露任何信息。在知道麦考密克死亡的消息以后，琼斯表示她怀疑凶手是巴哈。但是琼斯并没有提供任何细节来解释她为什么认为杀死麦考密克的人是巴哈。麦考密克并不一定是被巴哈亲手杀死的，也许这次巴哈找人代替了他。

警方的一名线人通知警方说，这起谋杀的凶手是格雷戈里·拉马尔·诺克斯（Gregory Lamar Knox）。诺克斯是当地一名毒贩，其地盘范围涵盖麦考密克居住的保障房小区。除了是麦考密克命案的嫌疑人以外，诺克斯还是其他多起谋杀案的嫌疑人。因此，警方线人的上述说法似乎

比较合理。警方发现，巴哈与诺克斯之间可能存在一些联系，但是警方掌握的两人之间的联系还不够强。尽管警方在侦查此案的过程中尽了力，但他们仍然未能找到足够的证据。最终，警方未能以谋杀麦考密克的罪名逮捕巴哈或者诺克斯（或者其他任何人）。

但是，麦考密克自己似乎能为警方提供更多线索。

麦考密克的尸体

1999年6月30日，一位女士在美国67号公路附近的一条野外道路上开车时，在玉米地附近发现了一具尸体，并报了警。虽然尸体已经有些腐烂，但是根据指纹可以确认死者就是41岁的里基·麦考密克。[注]麦考密克的尸体脸朝下平躺在野地里，发现尸体的地点在圣查尔斯县，距离麦考密克工作和居住的圣路易斯市中心地区大约有20英里的距离。麦考密克为什么会出现在这里？他是不是为了躲避麻烦而选择了离开圣路易斯呢？由于麦考密克本人存在健康方面的问题，所以也许他是自然死亡的。但是，他是如何到达这个地方的呢？如果他曾经沿途搭过车，那么为什么没有目击证人联系警方称自己开车搭载过他？如果他是先搭乘公共汽车然后再步行到达这个地点的话，那么为什么警方也没有找到可以支持这种说法的证据？但是，警方仍然没有排除麦考密克是因为健康问题而死亡的可能性。

1995年，在美国67号公路的同一路段附近的一间废弃的房屋中，曾经发现过一具女尸。据称这名女子生前是一名妓女。1995年发现的那具尸体绝对不是自然死亡，因为尸体几乎被子弹打成了筛子。2001年，在距离麦考密克尸体发现地点300码[注]的地方，又发现了两具裸体女性的尸体。那么1995年的案件和2001年的案件是否与麦考密克命案有联系呢？会不会是同一名精神变态者谋杀了这些女性和麦考密克呢？

由于暴露在野外的时间较长，麦考密克的尸体损毁程度比较高。虽

然麦考密克的死因可疑，但是在经过尸检以后，病理学家的结论是：“无法判断”麦考密克的死因。

在各种悬案中，经常会出现一些互相矛盾的说法，读到本章的这个地方，想必读者已经习惯这一点了。在本案中，也出现了一处关于麦考密克伤情的矛盾之处。6月30日，在麦考密克的尸体刚刚被发现时，警方称麦考密克的头部似乎受过伤。然而第二天，奥康纳却表示，由于尸体腐烂的情况过于严重，无法判断死者生前是否受过伤。

未被揭露的密码

虽然麦考密克的尸体由于腐烂程度太高已经无法为警方提供太多线索，但是在麦考密克的尸体上发现的两页密码却是清晰可辨的。一开始，警方选择不向公众透露发现的密码，然而在破译这份密码的过程中，警方却一直没有能够取得任何进展。圣查尔斯县治安官办公室的克雷格·麦圭尔（Craig McGuire）警官称，圣查尔斯县治安官办公室和重案组在案发后的一年内曾寻求过美国联邦调查局的帮助。

在此案发生时，美国联邦调查局的密码破译部门已经从华盛顿特区搬到了弗吉尼亚州的匡蒂科。圣查尔斯县治安官办公室认为麦考密克是死于谋杀，联邦调查局也同意这个意见。但是，虽然联邦调查局拥有很多密码破译方面的专家，他们却没有能够解开在麦考密克身上发现的那两页密码。

美国联邦调查局似乎非常喜欢搞一些“十大”列表，他们也有一份“十大未解密码”列表，而在麦考密克身上发现的那两页密码就在这份列表上。当时，在这份“十大未解密码”列表上，只有一种密码是公众熟知的，那就是我们在第5章中提到的黄道十二宫杀手密码。其他9种密码都是对公众保密的。

许多年过去了，美国联邦调查局一直没有能够破译麦考密克密码。

最终，他们在美国密码协会的全国会议上将麦考密克密码公布给了美国密码协会的所有会员。然而，在那以后，仍然没有人能够破译麦考密克密码。

接下来，联邦调查局决定进一步扩大征询范围，将麦考密克密码的内容公布给所有人。2011年3月29日，美国联邦调查局向公众公布了麦考密克密码的内容，并且提供了一些关于麦考密克命案的基本细节(注)：

> 1999年6月30日，密苏里州圣路易斯市警方发现了41岁的里基·麦考密克的尸体。麦考密克死于谋杀，尸体被扔在了野外。关于这起谋杀案的唯一线索是在死者的裤子口袋中发现的两页加密信息。
>
> 虽然密码分析与诈骗记录组的工作人员花了不少时间和精力来研究这两页密码，美国密码协会的成员们也为我们提供了帮助，但是直到今天，我们仍然未能解开这两页密码中的信息。而里基·麦考密克谋杀案至今也仍未告破。
>
> 密码分析与诈骗记录组的丹·奥尔森（Dan Olson）主任说："我们在密码破译方面的专业技能是过硬的，但是对于这则密码而言，我们仍然需要其他人的帮助。"
>
> 事实上，在密码分析与诈骗记录组的未破解密码清单上，里基·麦考密克身上的这两页密码是排名最靠前的密码之一。奥尔森说："如果能够破译这段密码，就有可能找出死者死前的行动细节，而警方就有可能根据这些线索侦破这起谋杀案。我们组会接到许多待破译的密码，但并不是每一段密码都能帮助警方侦破凶案。"
>
> 这段密码中有超过30行的内容使用了大量令人发狂的字母、数字、破折号，以及括号。麦考密克虽然没上完高中就辍学了，但他能够读书和写字，并且据说还颇具一些"街头智慧"。根据麦考密克家人的说法，他从童年开始就会使用这类密码，但是似乎他的家庭成员都不知道应该如何破译这段密码，而且我们也不清楚，除了麦考密克本人以外，是否还有任何其他人知道怎么翻译麦考密克发

明的这种秘密语言。警方的调查人员认为，麦考密克裤子口袋中的这两页密码应该写于他死前3天内。

在案发后的这些年中，密码分析与诈骗记录组的许多专家都对麦考密克密码的内容感到迷惑不解，这些人都是密码破译方面的专家，他们使用了一系列分析技巧来试图破译这段密码。奥尔森说："然而标准的密码分析程序用在这段密码上总是没有效果。"密码分析师对这段密码提出了若干种可行的理论，但是到目前为止，我们尚没有找出它的正确解法。

为了能够在破译工作上取得进展，专家需要麦考密克加密系统——或者类似加密系统的其他样本。这些样本也许能够为这段神秘的密码提供一些额外的上下文信息，或是让密码分析专家对两种不同的密码进行有意义的比较。如果找不到新的证据，奥尔森表示："也许某位能从创造性的角度看待事物的人能够为我们提供一些天才的新主意。"

这正是我们需要公众智慧的地方。这么多年以来，美国联邦调查局一直依靠公众提供的情报和其他协助来侦破罪案。虽然破译密码可能需要一些特殊技巧，但是你的帮助仍然有可能推动我们的侦破工作。请大家看一看麦考密克身上的这两页密码。如果你有关于破解这段密码的任何想法，或者见过与这段密码类似的其他密码样本，又或者有任何关于基里·麦考密克案的其他信息，请将上述内容通过以下这个网址发送给我们：http://forms.fbi.gov/code。或者，你也可以给联邦调查局的密码分析与诈骗记录组写信。他们的地址如下：

美国联邦调查局实验室

密码分析与诈骗记录组

调查大道2501号

匡蒂科，弗吉尼亚州，邮编22135

请注明：此信件与里基·麦考密克案有关

> 破译这段密码不会获得任何赏金，这只是一个挑战——如果你能破译这段密码的话，你将会获得一种满足感：你的脑力可能会帮助我们将一名凶手绳之以法。
>
> 奥尔森说：“即便这两页密码只是麦考密克写的一张购物清单或者一封情书，我们也想知道如何破译这种加密系统。这是一种我们完全不了解的密码系统。”

和之前提到的保罗·鲁宾案一样，关于麦考密克案的一些简单事实，各种媒体报道中也有许多互相矛盾的说辞。在美国联邦调查局发布的上述这封求助信中指出，密码是在“死者的裤子口袋中发现的”，但是一篇新闻报道则称：“在他（麦考密克）的衬衣口袋中，警方发现了两页加密的信息。”[注]

所以这两页密码究竟是在麦考密克的裤子口袋中发现的，还是在他的衬衣口袋中发现的呢？

此外，在美国联邦调查局的上述公开信中还提到，麦考密克“能够读书和写字”并且“根据麦考密克家人的说法，他从童年开始就会使用这类密码”。麦圭尔的说法与上述说法一致。麦圭尔说：“我们询问了麦考密克的家人，他们说，麦考密克常常会这么做。没有人知道这些密码究竟包含什么意思。这似乎是麦考密克书写私人日记的一种方式。”[注]

然而，一篇新闻报道却称：“麦考密克的家人说，他们从来不知道里基会用密码来写东西。麦考密克的家人称，他们只是告诉警方，麦考密克有时会写下一些无意义的文字，并把这种行为称作写作。并且他们认为麦考密克根本没有能力写出在他口袋中发现的那两页密码。”[注]美国联邦调查局在案发多年后才公布了这段密码，此时麦考密克的母亲才知道在儿子的尸体上发现过这两页密码。获知这一消息后，麦考密克的

母亲说：“除了他自己的名字以外，他什么也不会写。他从来没有用密码写过东西。”麦考密克的表亲查尔斯·麦考密克也说：“他不会拼写任何东西，他只会乱涂乱写而已。”

在考虑到以上所有情况之后，现在让我们来看看麦考密克的密码究竟长什么样。

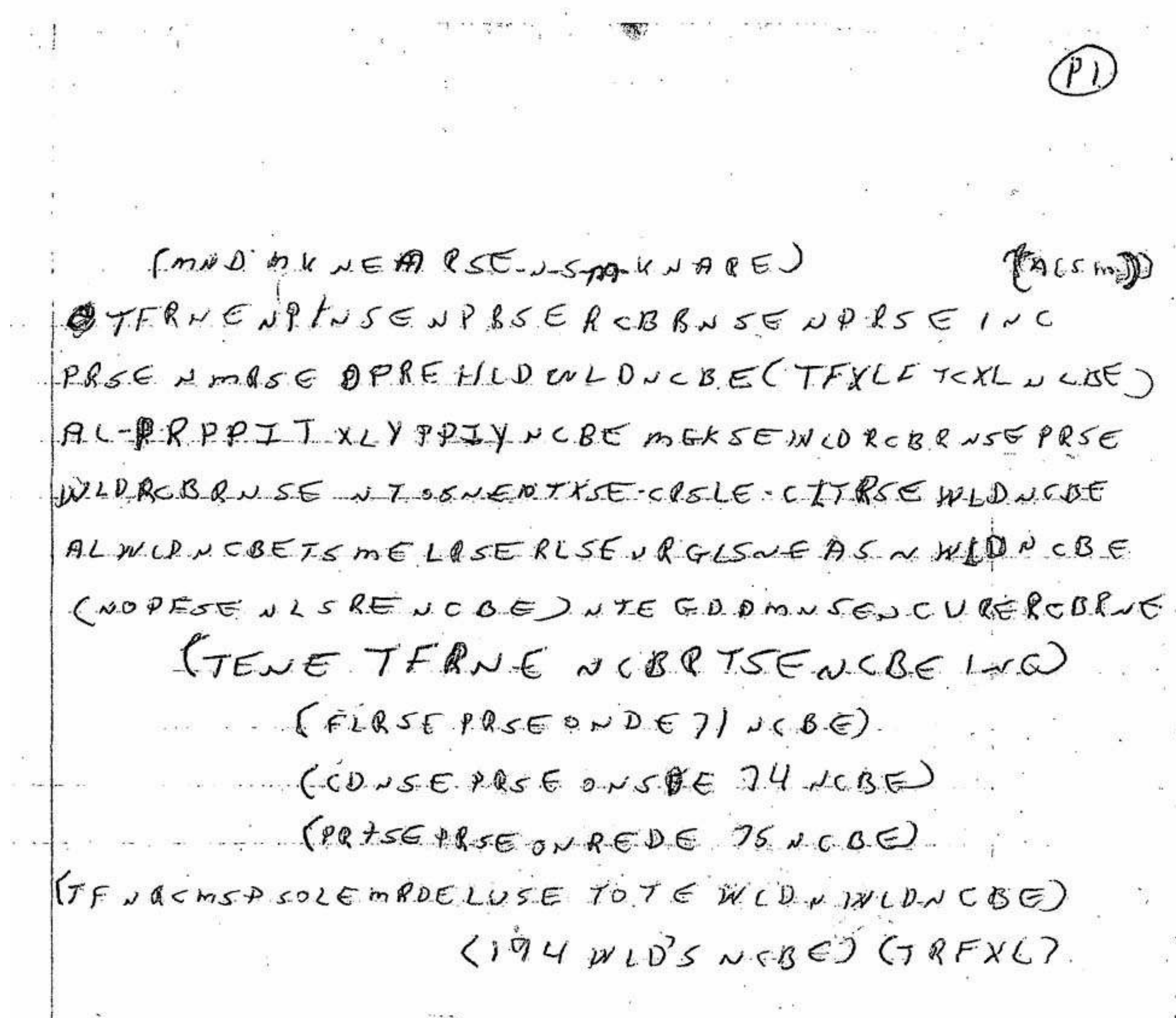


图6-27 麦考密克密码中的一页

本章中提到的3起案件不仅是按照时间顺序排列的，而且是按照《金发姑娘和三只熊》的顺序排列的。第一段密码中的字符数太少了，第二段密码中的字符数太多了，那么第三段密码呢？第三段密码中的字符数刚刚好。

图6-28 麦考密克密码中的另一页

这张纸条上的文字似乎包含某种秘密的语言，并且还使用了一些简化的谐音拼法。比如“MLSE”一词可能代表了“miles”（英里）这个单词。㊟

密码中还出现了“TRFXL”一词，一种较合理的解释是TRFXL = Traffic Light（交通信号灯）。此外，图6–27中的密码第1页的底部出现了“ WLD’S”一词。在正常英语中，字母S经常会跟在一个撇号后面。如果这段文字确实是某种密码的话，那么不管这种密码是替代密码

还是换位重排密码，撇号后面跟着任何一个其他字母的概率应该同样大。

那么，如果麦考密克的密码事实上是高度缩写的明文英文的话，我们究竟有没有可能读懂这些文字呢？这个问题的答案取决于这种高度缩写的英语中究竟缺失了多少字母。在萨默顿男子密码中，每个单词只保留了首字母，因此，我们不可能确定地找到唯一的正确解法——因为可能成立的情况太多了。然而，如果在麦考密克密码中，被省略的字母不到字母总数的一半，我们就应该能够读懂这段文字。这是因为，在英语中，大约有50%的字母是冗余的。让我们来考虑以下这个句子。在这个句子中，下划线所代表的字母被删除了。

T_E Q_I_K B_O_N F_X J_M_S _V_R T_E L_Z_ D_G.

原始信息一共包括35个字母，我删除了其中的14个，但是读者很有可能不用费太大力气就能读懂这句话。换句话说，只要在原始的35个字母中保留21个字母（即保留约60%的字母），就足够让读者看懂这句不完整的话了。

接下来，我要用另外几个例子来挑战读者的补缺能力。在下面这几个例子中，我分别删除了原始信息中不同百分比的字母。随着越来越高比例的字母被删除，你还能读懂这些信息吗？第一个例子比较长，这是为了帮助读者热热身！

删除25%的字母：

HER_’S TO _HE C_AZY _NES. _HE M_SFI_S. TH_ REB_LS. T_E TR_UBL_MAK_RS. T_E RO_ND P_GS I_ THE _QUA_E HO_ES. T_E ON_S WH_ SEE _HIN_S DI_FER_NTL_. THE_’RE N_T FO_D OF _ULE_. AND _HEY _AVE _O RE_PEC_ FOR _HE S_ATU_ QUO. _OU C_N QU_TE T_EM,

D_SAG_EE W_TH T_EM, G_ORI_Y OR _ILI_Y TH_M. AB_UT T_E ON_Y TH_NG Y_U CA_’T DO _S IG_ORE _HEM. _ECA_SE T_EY C_ANG_ THI_GS. T_EY P_SH T_E HU_AN R_CE F_RWA_D. AN_ WHI_E SO_E MA_ SEE _HEM _S TH_ CRA_Y ON_S, WE _EE G_NIU_. BEC_USE _HE P_OPL_ WHO _RE C_AZY _NOU_H TO _HIN_ THE_ CAN _HAN_E TH_ WOR_D, AR_ THE _NES _HO D_. – APP_E IN_.

删除25%的字母：

IF Y_U WA_T YO_R CH_LDR_N TO _E IN_ELL_GEN_, REA_ THE_ FAI_Y TA_ES. I_ YOU _ANT _HEM _O BE _ORE _NTE_LIG_NT, R_AD T_EM M_RE F_IRY_ALE_ – ALB_RT E_NST_IN

删除33%的字母：

MY _OU_TR_ IS _HE _OR_D, A_D M_ RE_IG_ON _S T_ DO _OO_ – TH_MA_ PA_NE

删除33%的字母：

I E_JO_ GE_TI_G P_OP_E A_GR_ AN_ GE_TI_G U_DE_NE_TH _HE_R S_IN, _SP_CI_LL_E_PL_ WH_ DO_’T T_IN_. – JE_LO _IA_RA

删除50%的字母：

I _O_’ T _O _R_G_. I _M _R_G_. – _A_V_D_R _A_I

删除50%的字母：

H_L_ O_ L_F_ I_ F_C_I_G U_, T_E _T_E_ H_L_ I_ D_A_I_G _I_H _T. – _E_R_ R_L_I_S

请读者注意，补全这些句子究竟要花费多长时间并不是我们要考虑的因素。即使要花上几个月的时间才能补全，只要这些句子能够被补全，那么句子中缺失的字母就是冗余的！

在某些情况下，只需要删除一个句子中数量占很小比例的字母，就会让句子的意思变得模糊。比如，让我们来考虑这样一个句子：ATTACK FROM THE _O_TH AT NOON.（中午时从“_O_TH”发动攻击。）原始句子中共有24个字母，而我只删除了其中2个。也就是说，删除字母后的句子中仍保留了91%的字母。然而，我们却没有办法知道攻击究竟是会从北方（NORTH）发动，还是会从南方（SOUTH）发动。

此外，我还可以用另外一个例子来说明，即使只删去原始信息中的很小一部分，也可能让我们完全无法搞清楚原始意思。这个例子是这样的：

MY FAVORITE MUSICIAN IS _ _ _ _ _ _ _ _ _ _ _ _.

（我最喜爱的音乐家是。）

在这个例子中，我删除了原始信息中的最后两个单词，长度分别是5个字母和6个字母。删除这些字母后的句子还剩下20个字母，也就是说，我们仍然能够看到原始信息超过64%的内容。在这个例子中，我们

显然可以找到补全这个句子的有意义的解法，但是我们永远无法确定究竟哪种解法才是这个句子的原意。

在麦考密克密码中，并没有这种下划线能告诉我们究竟哪些地方的字母被删除了。但是从另一个方面来看，破译麦考密克密码要比破译我举出的某些例子更简单，因为我们知道它的背景信息。在补全我所举出的这些例子中的句子时，我们没有任何背景信息可供参考。但是在麦考密克密码中，我们可以比较合理地假设，密码中会出现某个特定区域中的街道名称等信息。然而从另一个方面来看，麦考密克不仅省略了许多字母，还很有可能把许多单词拼错了，这就增加了破译这段密码的难度。但不管怎么样，我还是鼓励读者去破译麦考密克密码。如果能够看到不同的读者得出相似的解法，将会是一件非常有趣的事情。祝各位读者好运！

在本章开头，我向读者介绍了安东尼·鲍彻的短篇小说《QL696.C9》的大致情节。考虑到有些读者可能已经忘了这个故事，我有必要再简要复述一遍故事的主要内容：一名图书馆管理员坐在打字机前被枪杀。在生命的最后时刻，受害者在打字机上留下了一些奇怪的文字："QL696.C9"。随着调查的进行，警方将嫌疑人的范围缩小到了以下几个人之间：低级图书馆管理员斯特拉·斯威夫特，儿童图书馆管理员科拉·贾维斯，图书馆赞助人詹姆斯·斯蒂克尼，以及高中老师诺伯特·乌特。读者的任务是判断以上这些嫌疑人中究竟哪一位是真正的凶手。侦破此案的关键是找出图书馆管理员留下的这个书号究竟对应于哪个主题的书。经调查，"QL"代表动物学，6打头的分类是脊椎动物，"696"对应的具体类别是鸟类，而".C9"是雨燕目（swift）。因此，凶手是斯特拉·斯威夫特（Stella Swift）。当然，如果作者能够设计出一种既不需要死者背熟国会图书馆分类系统，也不要求死者花时间查阅这一系统的故事情节，那么这篇小说的答案就显得更加优雅迷人了。如果这个书号暗示的是凶手的名字，那这个凶手就一定是斯特拉·斯威夫特，因为其他几名嫌疑人的名字（Jarvis、Stickney、Utter）都与死者留下的书号没有任何联系。

1. Anthony Boucher, “QL696.C9.” Ellery Queen’s Mystery Magazine, May 1943.
2. Eye Doctor Guide.com, http://www.eyedoctorguide.com/Eye-Color/hazel-eyes-eye-color.html.
3. “Inquest into the Death of a Body Located at Somerton on 1.12.48.” [refers to Dec. 1, 1948], 1949, p. 69. Hands can tell us a lot about a person. In this instance, it was also noted that the hands were “hard, but were not rough from performing manual work.”
4. Gerald (Gerry) Michael Feltus, The Unknown Man: A Suspicious Death at Somerton Park (Rich-mond, Australia: Hyde Park Press, 2010), 143.
5. Feltus, The Unknown Man, 39–40.
6. Kerry Greenwood, Tamam Shud: The Somerton Man Mystery (Sydney, Australia: NewSouth Publishing, University of New South Wales Press Ltd., 2012), 28.
7. Descriptions vary slightly.
8. “Inquest into the Death of a Body,” 79.
9. All of the marks were on the pocket label of the same pair of pants.
10. “Inquest into the Death of a Body,” 81.
11. Feltus claims that the paper was rolled up. Greenwood described it as folded.
12. “Inquest into the Death of a Body,” 37.
13. “Inquest into the Death of a Body,” 39.
14. “Inquest into the Death of a Body,” 39.
15. “Inquest into the Death of a Body,” 41.
16. “Inquest into the Death of a Body,” 45.
17. “Inquest into the Death of a Body,” 47.
18. “Inquest into the Death of a Body,” 81.
19. “Inquest into the Death of a Body,” 85.
20. “Inquest into the Death of a Body,” 85.
21. “Inquest into the Death of a Body,” 85.
22. 索佛那（Sulphonal）即双乙磺丙烷，它同巴比妥酸盐都被用作安眠药。——译者注
23. “Inquest into the Death of a Body,” 95.
24. “Inquest into the Death of a Body,” 97.
25. “Inquest into the Death of a Body,” 97.

26. “Inquest into the Death of a Body,” 97.

27. “Inquest into the Death of a Body,” 9. Note: There are two Clelands involved with this case, Thomas and John. They were cousins.

28. “Inquest into the Death of a Body,” 9.

29. “Inquest into the Death of a Body,” 7.

30. Greenwood, Tamam Shud, 80.

31. The suitcase can be seen in the 1978 documentary at http://www.youtube.com/watch?v=nnPqlYPQ9lY, but it was destroyed in 1986.

32. “Inquest into the Death of a Body,” 73.

33. Feltus, The Unknown Man, 17.

34. Feltus, The Unknown Man, 171.

35. He wished to remain anonymous. His name is given as Ronald Francis in the books by Feltus and Greenwood, but this is a pseudonym. A list of common errors made by people writ-ing about this case states, “Reports sometimes refer to the man who found the copy of The Rubaiyat, tossed in the back of his car, as a ‘doctor’ or ‘chemist’. This is not certain. In fact both his name and real occupation have been withheld. Also the reason why his details are withheld is also suppressed. All we can assume is that he was some kind of professional.” From https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/List_of_facts_on_the_Taman_Shud_Case_that_are_often_misreported.

36. The Advertiser (Adelaide, South Australia), “Police Test Book for Somerton Body Clue,” July 26, 1949, p. 3.

37. Maybe. The 1949 inquest, p. 5, claims that the “Tamam Shud” paper came from a second edi-tion. In any case, by “first edition,” I mean the first from this publisher. It is not the first appear-ance of the book in print.

38. Some reports say “in the back of the book,” whereas others say “on the back of the book.” One official police document says that the back cover was missing.

39. “XXOO”是“抱抱亲亲”的意思。——译者注

40. If the hypothesis that follows is correct, this is exactly what we would expect. If the cipher consists of just initial letters, we should have a close match with initial frequencies, less of a match with overall frequencies (but not a total disconnect, since initial letters are included in determining overall frequencies), and a strong mismatch when comparing with terminal frequencies, since almost none of the initial letters are counted when compiling terminal fre-quencies — the only exceptions arise from the one-letter words A and I.

41. INRI是Iesus Nazarenus Rex Iudaeorum的缩写，意为“耶稣，拿撒勒人，犹太人的君

王”。在许多描绘耶稣被钉在十字架上的情景的油画中，十字架上都写着“INRI”的字样。——译者注

42. I redacted most of the editor’s phone number. Please e-mail him if you have the solution!

43. Simon Singh, The Codebook (New York: Doubleday, 1999).

44. Feltus believes that he found the entire correct solution, but he doesn’t reveal all of it in his book. Instead, he refers the reader to the back cover, which bears an image of the cipher. He also included a phone number alongside the cipher, but it’s a fake. That is, it doesn’t match the phone number that played an important role in the case.

45. 罗夏克墨迹测验是瑞士精神病学家罗夏克发明的一种人格测试。在罗夏克墨迹测验中，受测人会看到多张卡片上的墨迹图案，然后说出他觉得这些图案像什么。医生可以根据受测人的回答判断其性格。——译者注

46. Some proposed solutions, displayed on pages 119 and 120, are of the type I propose (taking cipher letters as the first letters of words), but there is no reason to favor them over many other potential solutions.

47. There are claims that more than one telephone number was present, but nothing authoritative enough to warrant inclusion here. This is another instance where we are greatly hampered because most of the police file is no longer available.

48. The term “nurse” may not have been technically accurate for the woman at this point in her life. See https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/List_of_facts_on_the_Taman_Shud_Case_that_are_often_misreported, item no. 4.

49. 这是《鲁拜集》中的一首诗，中文版来自黄杲炘1982年的译文。——译者注

50. Boxall’s copy was a 1924 Sydney edition.

51. Greenwood, Tamam Shud, 60.

52. “Inquest into the Death of a Body,” 7.

53. “Inquest into the Death of a Body,” 53.

54. Feltus, The Unknown Man, 151.

55. Feltus, The Unknown Man, 108.

56. Feltus, The Unknown Man, 178–79.

57. For more on early intelligence sharing with Australia, and a slightly different version of the story above, see Tom Johnson, American Cryptology during the Cold War: 1945–1989, Book I: The Struggle for Centralization 1945–1960 (Ft. Meade, MD: Center for Cryptologic History, National Security Agency, 1995), 18–19. Discrepancies are minor, such as labeling the cryptanalyst as being from SIS (Signals Intelligence Service) instead of ASA. There were frequent

name changes during these years. The evolution led to the National Security Agency (NSA) in 1952.

58. Wikipedia, http://en.wikipedia.org/wiki/Taman_Shud_Case, citing Phillips, John Harber, “So When That Angel of the Darker Drink,” Criminal Law Journal 18, no. 2 (April 1994): 110.

59. Wikipedia, http://en.wikipedia.org/wiki/Taman_Shud_Case.

60. Victor Navasky, ed., The Nation, New York, Commentary, “Harry Dexter White,” letter to the editor, April 1, 1988, available online at http://www.commentarymagazine.com/article/harry-dexter -white/.

61. On November 3, 1948, the day after Harry S.Truman defeated Thomas E.Dewey in the presi-dential election, the Chicago Daily Tribune ran the headline “Dewey Defeats Truman.” Actually, the Dewey presidency has more sources to back it up than the digitalis-induced death of White. The Journal of Commerce ran the headline “Dewey Victory Seen as Mandate to Open New Era of Government-Business Harmony, Public Confidence” on November 3.

62. 《芝加哥每日论坛报》1948年曾刊登过一条错误的头条消息，称杜威击败杜鲁门当选美国总统，实际上赢得该次大选的是杜鲁门。——译者注

63. Trove digitized newspapers, http://trove.nla.gov.au/ndp/del/article/76017408. Thanks to James Ramm for pointing this article out to me!

64. Greenwood, Tamam Shud, 122–23.

65. 来自黄杲炘1982年的译文。——译者注

66. 希思科特是珀斯郊区的一个地点，此处有一家精神病院。——编者注

67. 所谓“变得更加稳定”是自杀的委婉说法。——译者注

68. https://web.archive.org/web/20110612061900/http://www.weirld.com/Paranormal/UFOs -Aliens/The-Strange-Case-of-the-Somerton-Man-Time-Traveller-Human/Alien-Hybrid-or -Secret-Agent-Spy.html.

69. “Weirld” is not a typo but rather a portmanteau of “weird” and “world.”

70. America’s Most Wanted, http://en.wikipedia.org/wiki/America’s_Most_Wanted#Profiling – missing–persons. The man was captured in April 2008.

71. Unsolved Mysteries, https://web.archive.org/web/20140422010517/http://unsolved.com/about.html.

72. Greenwood, Tamam Shud, 129.

73. Available online at http://www.youtube.com/watch?v=iy5s50F3uB8 (“Somerton Man” seg-ment). This is the source of the quotes that follow.

74. Some secondary sources say “formaldehyde,” but that is technically wrong, as it refers to a

gas.However, “formaldehyde solution” is equivalent to formalin, which is a mix of formaldehyde gas and water.

75. Renato Castello, “New Twist in Somerton Man Mystery as Fresh Claims Emerge,” Sunday Mail(SA), November 23, 2013.

76. Castello, “New twist.”

77. Castello, “New twist.”

78. Gerry Feltus, “Second Application to Exhume Refused - 4 Jun 2014,” http://theunknownman.com/comments.html This opinion also appeared at Pete Bowes, “the dead will not arise .....Rau, his second ruling,” June 26, 2014, http://tomsbytwo.com/2014/06/26/the-dead-will-not-arise-rau-his-second-ruling/.

79. Kynton Grace, “South Australia’s X-Files: Part 2—The Somerton Man Mystery and the Secrets of Adelaide’s Tunnels,” The Advertiser, June 9, 2014.

80. “Dad Identifies Poisoned Youth as N.Y. Student,” Washington Times-Herald, January 22, 1953,p. 3.

81. “Body Found at Airport, Coded Note on Abdomen,” January 21, 1953.

82. “Code Note Taped to Body in Ditch,” The Evening Bulletin, Philadelphia, 1, column 2, Sports Final edition, January 20, 1953.

83. “Cyanide Caused Death at Airport,” The Evening Bulletin, Philadelphia, p.1, column 3, Post-script edition, January 21, 1953.

84. “Cyanide Caused Death at Airport.”

85. “Mystery Man at Airport Is Found Dead of Poison,” The Philadelphia Inquirer January 21, 1953,p. 1.

86. “Mystery Man Cyanide Clue Hints.” Murder Most accounts just say “cyanide.” Potassium cya-nide is specified in “Man Poisoned, Paper in Code Taped to Body; FBI Called In,” Washington Star, p. A-26, and in some other articles. It is “potassium or sodium syanide [sic]” in “Code Message Found Taped to Dead Man,” Washington Times-Herald, January 21, 1953, p. 35.

87. “Mystery Man Cyanide Clue Hints Murder.”

88. “Mystery Man Cyanide Clue Hints Murder.”

89. “Code Note Taped to Body in Ditch,” The Evening Bulletin, Philadelphia, January 20, 1953, p. 1.

90. “Body with Code Note Found Here,” Daily News, Philadelphia, January 20, 1953, p. 2.

91. “.‘Dulles’ Name Taped to Body of ‘Suicide,’” Washington Post.

92. “Code Message Found Taped to Dead Man,” Washington Times-Herald, January 21, 1953, p. 35.The quote is attributed to Dr. Edward Burke of the police crime laboratory, in “Mystery Man Cyanide Clue Hints Murder.”

93. We also have the quote “Police said they found no cyanide container near the body.” in “Cya-nide Caused Death at Airport.”

94. “Test Tube Found at Site of Airport Ditch Death,” The Philadelphia Inquirer, January 23, 1953,p. 28. Available online through http://fultonhistory.com/Fulton.html.

95. “.‘Dulles’ Name Taped to Body of ‘Suicide.’.” Also stated in “Student Identified as Cyanide Vic-tim,” New York Times, January 22, 1953.

96. “Mystery Man Cyanide Clue Hints Murder.”

97. “Code Note Taped to Body in Ditch,” The Evening Bulletin, Philadelphia, January 20, 1953, p. 1.Described as eight inches by three inches in “Code Message Found Taped to Dead Man,” Wash-ington Times-Herald, January 21, 1953, p. 35. It was described as only five inches in “.‘Dulles’ Name Taped to Body of ‘Suicide.’.”

98. E-mail from David Hatch to the author, October 3, 2012.

99. “Mystery Man at Airport Is Found Dead of Poison.” Another source claims that there was no wallet! See “Code Message Found Taped to Dead Man.”

100. “Body Found at Airport, Coded Note on Abdomen.”

101. “Cyanide Caused Death at Airport.” Some sources only mention “a car key.” Were there four keys or just one?

102. “Code Message Found Taped to Dead Man.”

103. “Codes Seen Key in Airport Death,” January 22, 1953.

104. For false report, see “Codes Seen Key in Airport Death.”

105. “Mystery Man Cyanide Clue Hints Murder.”

106. Rubin’s age was typically reported as eighteen, but some articles gave his age as nineteen. See “Body at Airport Is Identified as NYU Student,” Philadelphia, January 21, 1953, and “Airport Death Called Murder by Ominsky,” Philadelphia, January 21, 1953. In this second article, Rubin’s age is later stated as eighteen.

107. “Youth Dabbled in Cryptography,” Philadelphia Evening Bulletin, January 22, 1953.

108. In most accounts, it was forty-seven cents. For example, see “Code Note Taped to Body in Ditch.” But it was forty-six cents in “Body with code note found here.”

109. “Poison Victim Identified as N.Y. Youth,” The Philadelphia Inquirer, January 22, 1953, p.1, illus-trated on p. 3 and continued on p. 13, quote from p. 13.

110. “Poison Victim Identified as N.Y. Youth,” quote from p. 13.

111. “FBI Investigates Possibilities of Murder in Mysterious Cyanide-Death of Student,” Schenectady Gazette, January 22, 1953.

112. Jay Apt, “Note Baffles Decoders in Poison Death,” Daily News, January 22, 1953, p. 2.

113. “FBI Investigates Possibilities of Murder in Mysterious Cyanide-Death of Student.”

114. “Hazing Studied in Airport Death,” The Philadelphia Inquirer, January 28, 1953, p. 5.

115. “Student Identified as Cyanide Victim,” New York Times, January 22, 1953.

116. E-mail from Claire Ashley Wolford, May 2, 2012.

117. “Life on the Newsfronts of the World, Student Leaves a Coded Clue to His Death, a Soldier Plants a Flag and Flu Virus Sweeps the World,” Life, February 2, 1953, p. 30.

118. “Youth Dabbled in Cryptography.”

119. “Poison Victim Identified as N.Y. Youth,” quote from p. 13.

120. “Mystery Shrouds Death by Cyanide,” The Philadelphia Inquirer, March 25, 1953, p. 19.

121. “Mystery Shrouds Death by Cyanide.”

122. “Mystery Shrouds Death by Cyanide.” The names Edwin and Edward both appear in newspaper accounts.

123. “Body at Airport.”

124. “Body at Airport.”

125. “Gay rights campaigner calls for fresh inquiry into death of Alan Turing,” Manchester Evening News, December 24, 2013, http://www.manchestereveningnews.co.uk/news/greater -manchester-news/codebreaker-alan-turing-gay-rights-6445286, accessed July 11, 2014.

126. Langen, Harry [sic — it should say Henry], My Life Between the Lines.

127. Langen, My Life Between the Lines.

128. I found this paper as a clipping in an uncatalogued portion of the National Cryptologic Muse-um’s collection. It is not clear from the clipping which paper it came from!

129. Wolfram Alpha, http://www.wolframalpha.com/input/?i=average+english+word+length. You may find much larger estimates, but these simply average the lengths of all English words from some list. They do not weight the average by frequency. That is, the value above looks at actual usage.

130. Shane Anthony, “From 1999: Body found in field puzzles police,” St. Louis Post-Dispatch, July 2, 1999, but Christpher Tritto implied that the sentence was about two years in his article.

131. According to Christopher Tritto. Shane Anthony reported that he served 11 months.

132. Christopher Tritto, “Code Dead: Do the encrypted writings of Ricky McCormick hold the key to his mysterious death?” Riverfront Times (St. Louis), June 14, 2012.

133. Tritto, “Code Dead.” This article reports that “At least one gas-station employee” claims to have seen McCormick there that day. There’s no elaboration concerning the uncertainty expressed in the number of witnesses.

134. Anthony, “From 1999.” This article actually says “Highway 367,” but it’s a typo, one that has spread to the Wikipedia page for the McCormick cipher.

135. 1码≈0.9米。——编者注

136. Still available online at the FBI site, http://www.fbi.gov/news/stories/2011/march/cryptanalysis _032911.

137. Jennifer Mann, “FBI wants public to help crack code in St. Charles County cold case,” St. Louis Post-Dispatch, March 31, 2011.

138. Mann, “FBI wants public to help.”

139. Tritto, “Code Dead.”

140. Tritto, “Code Dead.”

141. 在《金发姑娘和三只熊》的故事中，金发姑娘来到三只熊的家里，她看到了三碗粥，第一碗太烫了，第二碗太凉了，第三碗温度刚刚好。后来她又看到了三张床，第一张太硬了，第二张太软了，第三张硬度则刚刚好。——译者注

142. Tritto, “Code Dead.”